THE COMMAND OF THE TREND:

SOCIAL MEDIA AS A WEAPON IN THE INFORMATION AGE

BY

JARRED PRIER

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2017

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

COL. SHAWN T. COCHRAN, PH.D. (Date)

JAMES M. TUCCI, PH.D. (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Jarred Prier received his commission through AFROTC from the University of Missouri in 2003. He is a Senior Combat Systems Officer with over 1,200 hours in the B-52H. Major Prier began his Air Force career as a Space Surveillance and Missile Warning Operations Crew Commander. He then completed Combat Systems Officer and Electronic Warfare Training at Randolph AFB, Texas. Following B-52H qualification training, he proceeded to Minot AFB; his work there culminated as an evaluator and the Wing Weapons Officer.

Before his developmental education and SAASS, he was a joint staff officer assigned to United States Strategic Command. In the academic year 2015-2016, he was an Air Force Foreign Policy Fellow at the Institute for the Study of Diplomacy within Walsh School of Foreign Service at Georgetown University. In addition to his Georgetown Fellowship, he served in the West Africa Office of the Bureau of African Affairs at the Department of State.

Major Prier holds an Interdisciplinary Bachelor of Arts degree in History, Religious Studies and Political Science from the University of Missouri, and a Master of Science in International Relations from Troy University.

ACKNOWLEDGMENTS

I would like to acknowledge several people without whose support and help I would have never have gotten off the ground with this study. First, I must again thank those who were so helpful with my fellowship research, which was the genesis of this work. Lee Brenner was instrumental in much of the early research I did on the topic. Lee, the former host of "Politics Powered by Twitter" on SirusXM POTUS channel, was kind enough to help me get started with an interview and included me in a cyber think-tank for the study of ISIS activity on social media. Additionally, I am still thankful to Georgetown University Professor Shanthi Kalathil and USAF POLAD, Mr. Matthew Weiller, for graciously reviewing the work on my original project. Once again, I am also grateful to my friend Sarah McCammon, who provided personal insight over the past two years from a journalist's perspective, despite her chaotic schedule traveling the country covering the Trump campaign.

My appreciation also goes back a decade to my friend who created a MySpace account for me in 2007 despite my strong objections. At only 12 years old, she was convinced that social media was the future of communication. I could not understand it at the time, but had I not caved to her millennial way of thinking, I would have never taken an interest in this topic.

From SAASS, Dr. Wright always provided kind and encouraging words as he helped me become a better writer. I also want to thank Dr. Chiabotti, who encouraged me to continue my work on this topic. Dr. Benson and Dr. Tucci both provided outstanding feedback, and I am very grateful for all of the guidance that Col. Cochran has given me to shape this project.

Finally, and most importantly, I want to express my sincere appreciation to my wife for her love, patience, and understanding during those times when I was absent in spirit, off struggling with this paper. Her presence was very important to me and made all the difference in ensuring my success in completing this work.

PREFACE

I spent the 2015 academic year as an Air Force Foreign Policy Fellow with the State Department and Georgetown University. I used part of my fellowship to research and write on a topic that most in Washington agreed was an important issue, but few could describe the link between violent extremism and social media. Leaders in the Pentagon, the NSC, and the State Department would wax poetic that *we* had to "fight them on social media," and *we* had to "change the narrative" to win the Twitter war with ISIS. I quickly realized that most of the people advocating that position knew some things about ISIS but absolutely nothing about social media.

Ultimately, my paper was a rebuke of the social media methodologies of the United States government at the time. The State Department attempted to create an expensive social media ad campaign to find ISIS Twitter accounts and essentially argue with them on the finer points of their religion. Meanwhile, ISIS was using an impressive combination of high- and low-tech solutions to dominate social media. Put simply, ISIS was using others to spread their message for them—including the unwitting Western media. That paper's thesis thus became: *we* should use their playbook. I have revised and included a small portion of that research in this paper.

Around the time I started my research, I read an article in *The New York Times* about a professional network of internet "trolls" in Russia. An internet troll is someone who writes—typically on social media and in news comment sections—for the exclusive purpose of creating mischief. Trolls are usually rude, vulgar, and have no regard for conversation. Their only goal is to insert their opinion aggressively into the discussion. The Russian government, according to the article, hired the trolls to create panic and distrust in the institutions of the United States.

Shortly after I read the article, my undergraduate alma mater, the University of Missouri, went through a difficult period of racial strife on campus that generated significant media attention. I began to recognize some of the techniques of the Russian trolls from the *Times* article. I took note of particular Twitter handles to monitor over the next several months. Over time, I watched as the Russian troll network morphed from one event to another. It changed so dramatically that I nearly changed my research topic to write on that evolution alone. With the political morphing, I also noticed a slight change in techniques. They too had learned from ISIS and were unleashing a cyber-attack that few—if anyone—ever anticipated.

I continued on my personal Twitter quest to monitor the trolls and their techniques throughout the election. I have seen several dark places on Twitter. After clicking through several leads, I sometimes felt as if I was in a dark place surrounded by soulless, faceless demi-humans spouting hate and lies robotically. In some cases, it was a Twitter "bot."

The topic of Russian interference in the election is controversial, and clearly, it has been framed as a partisan issue. I do not believe that it should be a partisan issue, and this paper will not fall on a side of the election. To be certain, President Trump's campaign benefited from the Russian influence operation, but the fact that the issue has taken an ugly partisan slant on both sides is exactly the goal of any troll, particularly the Russian cyber warriors.

I cannot fully elaborate on all of the psychological, sociological, or even technological details with influence. My intent is to highlight how an adversary uses social media to manipulate the American public. Until the public and our leaders understand the true nature of social media manipulation, Russia will likely continue to exploit that vulnerability, and other adversaries will attempt to use the same methods.

ABSTRACT

This study demonstrates how social media is a tool for modern warfare in the information age. The report builds on analysis of three distinct topics: social networking, propaganda, and news and information sharing. Two case studies are used to show how state and non-state actors can use social media to employ time-tested propaganda techniques to yield far-reaching results. The spread of the propaganda message is accomplished by tapping into an existing narrative, then amplifying that message with a network of automatic "bot" accounts to force the social media platform algorithm to recognize that message as a trending topic. The first case study analyzes ISIS as the non-state actor, and the second observes Russia as the state actor, with each providing evidence of successful weaponizing of social media. The paper concludes that weaponization of social media will continue to be a decisive factor in future warfare as more countries attempt to build influence operations on social media in the same way Russian operators conducted information warfare against the United States in the 2016 Presidential Election.

CONTENTS

Illustrations

Table

Illustrations

Figure

Introduction

> *The battlefield can no longer be limited; it now extends to all the lands and seas of all the nations in the war. No longer can a line of demarcation be drawn between belligerents and nonbelligerents, because all citizens wherever they are can be victims of an enemy offensive.*
>
> Giulio Douhet, 1928

For years, analysts in the defense and intelligence communities have warned lawmakers and the American public of the risks of a cyber Pearl Harbor. The fear of a widespread cyber-based attack loomed over the country following intrusions against Yahoo email accounts in 2012, Sony Studios in 2014, and even the United States Government (USG) Office of Personnel Management (OPM) in 2015. The average American likely did not understand exactly how, or for what purposes, US adversaries were operating within the cyber domain; but the consequences of future attacks were not difficult to imagine.

According to experts, enemies of the United States could target vulnerable power grids, stock markets, train switches, academic institutions, banks, and communications systems in the opening salvos of this new type of warfare.[1] But what may have been the most signifiant cyber-attack on the United States was neither a brute-force strike typically associated with warfare nor a massive theft of money or data. In fact, hacking was only a minuscule part of a cyber operation designed by Russian agents to affect the United States Presidential election of 2016.[2]

---

[1] Elisabeth Bumiller, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." The New York Times. October 11, 2012.
[2] Office of Director of National Intelligence. Report: "Assessing Russian Activities and Intentions in Recent US Elections." January 6, 2017.

Instead, this operation was characterized by the insidious exploitation of existing social media sites.

This paper analyzes the weaponization of social media by US adversaries, including both state and non-state actors. Social media sites like Twitter and Facebook employ an algorithm to analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity. For users, the trend list is a quick way to review the most discussed topics at a given time. And according to a 2011 Cornell University study on social media, a trending topic "will capture the attention of a large audience for a short period." The trend list thus "contributes to agenda setting mechanisms."[3] Utilizing existing online networks in conjunction with automatic "bot" accounts, foreign agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate the message faster and cheaper than through any other medium in history. I argue that in contrast to more traditional forms of cyber-attack, US adversaries now seek to control and exploit the trend mechanism on social media to harm US interests, discredit public and private institutions, and sow domestic strife. Such efforts represent a relatively novel and increasingly dangerous means of weaponizing social media, which I label *Command of the Trend*.

The New Battlefield

Command of the trend requires few resources and minimal technical skill. Both state and non-state actors outside the United States can access regular streams of online information via social media to influence networked groups within the United States. Thus, instead of attacking the military or economic infrastructure, cyber operations now

[3] Sitaram Asur, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang. "Trends in Social Media: Persistence and Decay." (Cornell University, 2011), 1.

target the people within a society, influencing their beliefs as well as behaviors, and diminishing trust in the government and public institutions.

This concept, at its core, is similar to a theory proposed by Italian air power theorist, Giulio Douhet. In his post-World War I book, *The Command of the Air,* Douhet posited that air power would fundamentally change warfare because of its unique capability to bypass the bloody stalemate of land combat and bring warfare directly to the enemy citizen. According to Thomas Hippler, who analyzed Douhet's theory in *Bombing the People*, the most important theme "and the one on which Douhet insists on several occasions" is the "nationalization of war."[4] In a democracy, the will of the people dictates the actions of the government. Therefore, the potential for direct attacks against the population will lead to fewer wars because, "people will not be able to say anymore: 'Let us all arm for war, but you go and do the fighting.'"[5]

Given the destructiveness assumed with industrial-age air power theory, it is ironic that current expectations for air strikes involve minimal civilian casualties. Because of this sensitivity, adversaries like al-Qaeda have been quick to use images of civilian casualties—including fake and misidentified pictures of dead bodies—as propaganda against the United States. Images shared via social media networks have proven valuable for both demonstrating US incompetence and recruiting new fighters. One such recruit was Arid Uka, an Albanian Muslim living in Germany, who killed two US military members at a Frankfurt airport in 2011 after watching highly edited YouTube videos of Americans allegedly committing atrocities against Muslim civilians.[6]

---

[4] Thomas Hippler, *Bombing the People: Giulio Douhet and the Foundations of Air-power Strategy, 1884-1939*. (Cambridge Military Histories, 2013), 85.
[5] Douhet, 196.
[6] Gabriel Weimann, *Terrorism in Cyberspace : The next Generation*. (Washington, D.C.: Woodrow Wilson Center Press, 2015), 125.

Stories like that of Arid Uka are well known. The "self-radicalized" jihadist spends time on various social media networks, watching videos and reading religious teachings, eventually coming to a point where he or she is willing to commit a terrorist act. Perhaps no group has used social media to recruit as effectively as the Islamic State of Iraq and Syria (ISIS).[7] Using a variety of platforms, ISIS has shown that "social media can compensate for the disadvantages of undisciplined groups by reducing the costs of coordination."[8] Beyond recruitment and coordination, ISIS has also demonstrated the viability of social media as a propaganda-spreading machine, which was certainly not the original purpose of networking websites.

The adaptation of social media as a tool of modern warfare should not be surprising. According to Douhet, "technology must adapt itself to the needs of war, and not the needs of technology."[9] Internet technology evolved to meet the needs of information-age warfare around 2006 with the dawn of Web 2.0, which allowed internet users to create content instead of just consuming online material. The social nature of man ultimately led to virtual networking. As such, traditional forms of media were bound to give way to a more tailorable form of communication, and US adversaries were quick to find ways to exploit the openness of the internet, eventually developing techniques to employ social media networks as a tool to spread propaganda.

That said, it is worth noting Eric Hoffer's comments that "propaganda on its own cannot force its way into unwilling minds, neither can it inculcate something wholly new."[10] For propaganda to function, it needs a previously-existing narrative to build upon, as well

---

[7] The Islamic state is sometimes referred to as IS, ISIS, ISIL or Daesh. For simplicity, this paper will refer to the group as ISIS unless a quote uses a different term for the group.
[8] Clay Shirky, "The Political Power of Social Media." *Foreign Affairs*. December 20, 2011.
[9] Hippler, 46.
[10] Eric Hoffer, *The True Believer; Thoughts on the Nature of Mass Movements.* (New York: Harper and Row, 1951), 105.

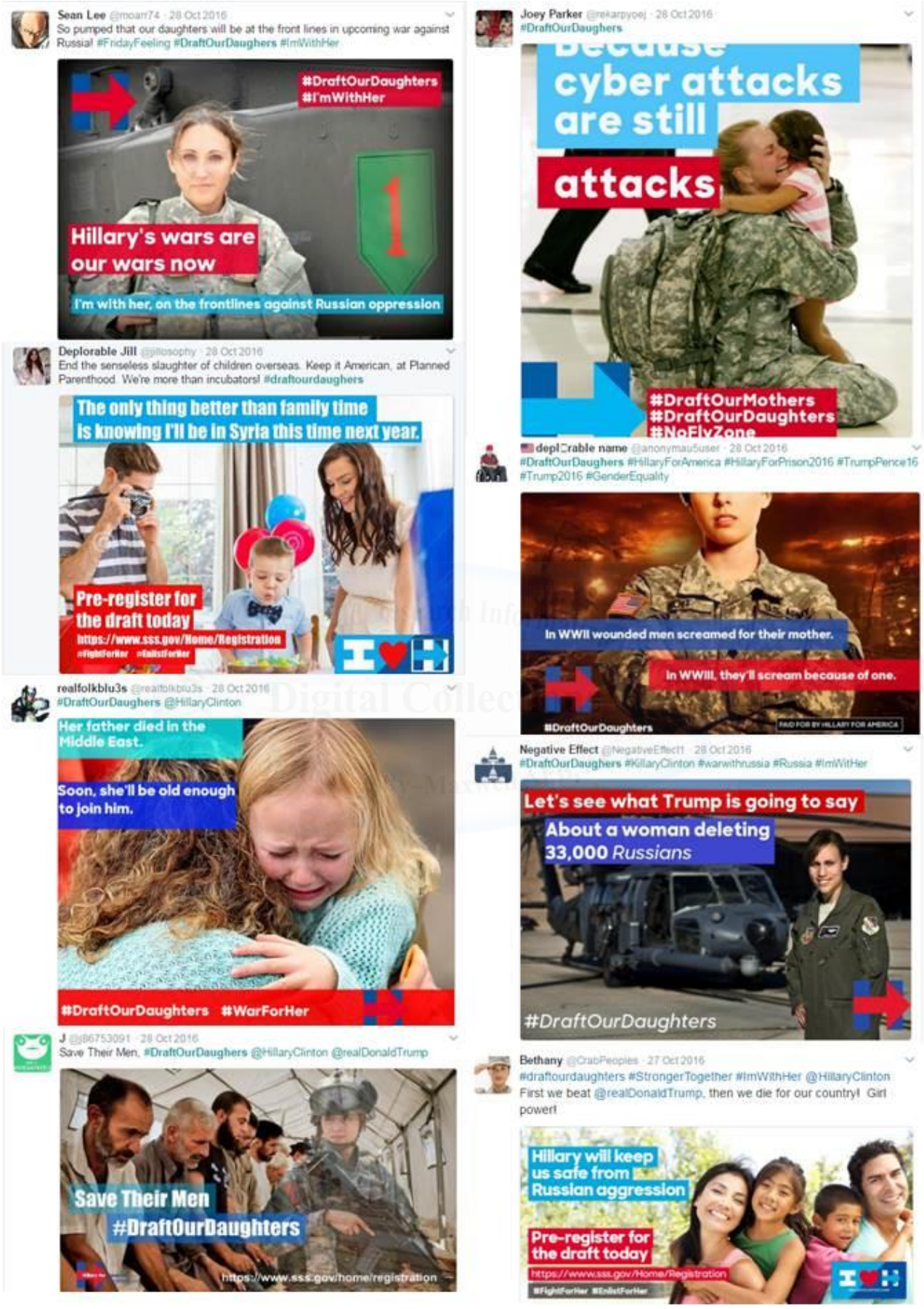


Figure 1. Fake advertisements associated with a Twitter trend
Source: Author created compilation of Twitter screenshots, October 2016

For example, Figure 1 shows various images that trended on October 28, 2016, using the hashtag #DraftOurDaughters. The basis of the hashtag was an actual news story on Presidential candidate Hillary Clinton's support for including women in Selective Service. A well-choreographed campaign took the article and added a realistic-looking campaign advertisement using graphics and font associated with the Clinton campaign. The pictures on those fake advertisements used stock images available for free using a Google Image search. The accounts sending out those images attached the hashtag using two different approaches: acting as supporters of Clinton who wanted to draft women to "go to war with Russia," and posing as people opposed to Clinton and her purported plans. Sometimes a single account would send tweets acting as both a supporter and opponent, with each tweet employing the same hashtag in order to induce a trend. Additionally, some of the tweets included other trending topics to maximize viewing across several trends. The images inspired a variety of interactions based on the political leanings of the viewer, but each discussion kept the trend going. Ultimately, the trend spread to a worldwide audience even though the underlying message was fake. Based on an identifiable pattern, it appears an army of Russian "trolls" and bot accounts worked in concert with a network of Americans to spread the disinformation.

Command of the trend hinges on four factors:

1. A message that fits an existing, even if obscure, narrative
2. A group of "true believers" predisposed to the message
3. A relatively small team of agents or cyber warriors
4. A network of automated "bot" accounts

The existing narrative and the true believers who subscribe to it are endogenous, so any propaganda must fit that narrative to penetrate the network of true believers. Usually, the cyber team is responsible for crafting the specific message for dissemination. The cyber team then generates videos, memes, or fake news, often in collusion with the true

believers. To achieve the effective spread of propaganda, the true believers, the cyber team, and the bot network combine efforts to take command of the trend. Going forward, this paper will explore the four factors associated with command of the trend, factors which together facilitate the weaponization of social media.

Structure

Again, I argue that foreign actors now seek to control and exploit the trend mechanism of social media to harm US interests and sow domestic strife. In support of this claim, the remainder of the paper is divided into four chapters. Chapter 1 provides a basis for understanding the weaponization of social media via command of the trend. It begins with definitions of social media and an analysis of social media as a tool for both obtaining and spreading information. It then looks more specifically at how US adversaries can utilize social media to target US citizens with malicious propaganda.

The next two chapters provide evidence of how non-state and state actors alike weaponize social media to counter the United States. The first case study covers ISIS from 2014-2016 to include an examination of the group's use of social media for recruiting, spreading propaganda, and proliferating terror threats. Chapter 3, the second case study, describes Russian hacking, espionage, disinformation, and manipulation of social media as related to the United States election of 2016. Evidence for this second case study comes from nearly two years of watching the activity of Twitter accounts believed by the author to be part of a Russian information warfare network.

Douhet concluded *The Command of the Air* with a fictional account of his prediction for the next war. Similarly, Chapter 4 of this study provides analysis and predictions of how the weaponization of social

media will continue to develop and what it will look like in the future. The paper concludes with a discussion of how the United States can respond to the growing threat of adversaries who seek to harm US interests and foster domestic instability through command of the trend.

Chapter 1

From a Place for Friends to the Nexus of Cyber Warfare

Young people don't want to rely on a God-like figure from above to tell them what's important. And to carry the religion analogy a bit further, they certainly don't want news presented as gospel. Instead, they want their news on demand, when it works for them. They want control over their media, instead of being controlled by it. They want to question, to probe, to offer a different angle.

Rupert Murdoch, 2005

In 2006, *Time* named "You" the person of the year because the increase in user-based internet content such as social media, online video sharing, and wikis made the internet "a tool for bringing together the small contributions of millions of people and making them matter."[1] The internet had evolved from a point when a user could only receive information, to the point where the average user could create new content. Once this happened, networks of people began to form online. The human desire to be a part of a crowd began to manifest itself virtually with the coming of "Web 2.0."

Long before the internet, German Nobel Prize Laureate Elias Canetti described the power of the crowd as being a shelter from danger and an escape from loneliness. Canetti believed that "nationalism, extremism, the yearning for democracy are all the products of crowd formations and thus manifestations of seeking to escape from

[1] Lev Grossman, "You — Yes, You — Are TIME's Person of the Year." *Time Magazine*, December 25, 2006.

loneliness."[2] Moreover, according to Kaplan, in modern times the need to be part of a crowd is "alleviated by Twitter and Facebook, [which] ultimately leads to the breakdown of traditional authority and the erection of new kinds."[3]

Media mogul Rupert Murdoch recognized the significance of the way people received their information when he purchased the MySpace social networking website in 2005. He noted that people no longer had to wait for information or even to have information delivered to them. Instead, the individual could decide what was important and only read what was important on demand. Not only could users select what news they want to see, but they could also use the medium to create news based on their opinions.[4]

This chapter covers the evolution of social media from "a place for friends," as the MySpace motto proclaimed, to a place to spread ideas and information. As such, social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare. Going forward, we examine social media terms and definitions, including the important concept of the social media trend, and look briefly into the fundamentals of propaganda. This chapter concludes by examining the spread of news on social media, specifically, the spread of "fake news" and the penetration of propaganda into mainstream media outlets.

Social Networks and Social Media

[2] Robert D. Kaplan, *Revenge of Geography*. Random House. Kindle ebook. 2012: 2,140
[3] Kaplan, 2,140
[4] Jeremy Scott-Joynt, "What Myspace means to Murdoch." BBC News Analysis. http://news.bbc.co.uk/2/hi/business/4697671.stm. July 19, 2005.

As social media usage became more widespread, users became ensconced within specific, self-selected groups, which meant that news and views were shared nearly exclusively with like-minded users. In network terminology, this group phenomenon is called homophily. More colloquially, it reflects the concept that "birds of a feather flock together." Homophily within social media creates an aura of expertise and trustworthiness where those factors would not normally exist. Ultimately, this "echo chamber" can promote the scenario in which your friend is "just as much a source of insightful analysis on the nuances of U.S. foreign policy towards Iran as regional scholars, arms control experts, or journalists covering the State Department."[5]

Homophily is nothing new. Politics, religion, and cars, as the old saying goes, have always been off-limit topics for polite conversation amongst strangers. This sound advice is based on the principle that such topics engender deeply-rooted beliefs with strong ties to emotions, and people have always tended to bond with those who think alike while rejecting the ideas of those they do not—especially with regards to politics. During the 2008 Presidential election, Valdis Krebs' consulting firm reviewed data from Amazon book sales. The results (see Figure 2) indicate that people only bought Republican-leaning or Democrat-leaning books—there was no overlap in book sales.[6]

[5] Tom Hashemi, "The Business of Ideas is in trouble: Re-injecting Facts Into a Post-truth World." *War on the Rocks*. December 9, 2016.
[6] Charles Kadushin, *Understanding social networks: Theories, concepts, and findings*. (New York: Oxford University Press, 2012), 7.

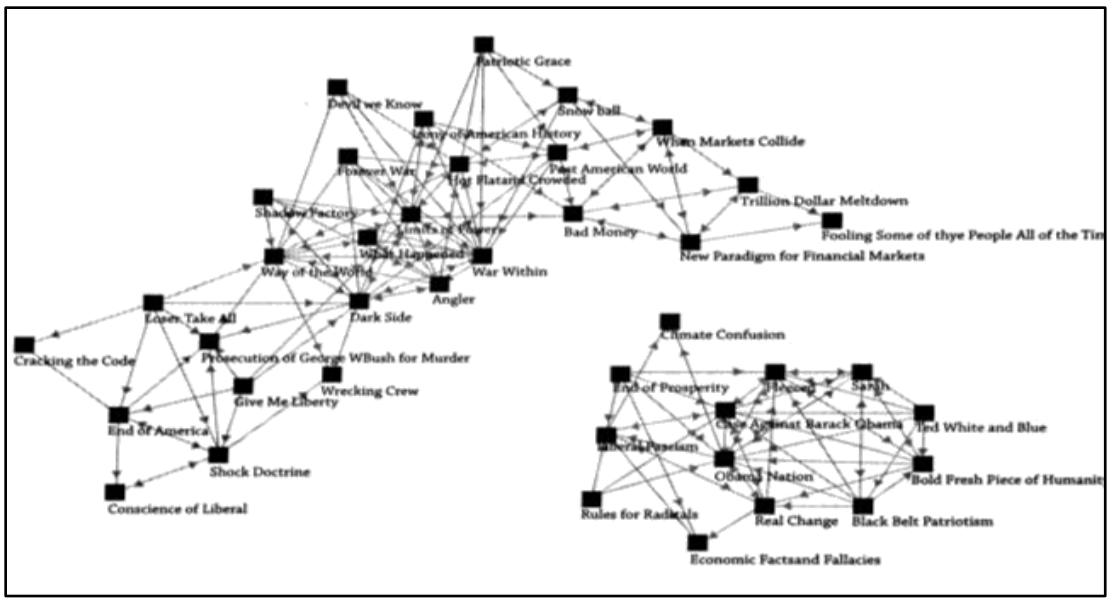


Figure 2. Books bought by the same people during 2008 election.
Source: *Understanding Social Networks*, Kadushin

The clusters of book sales represent networks. Social media allows the people who make up those networks to reach out and discuss politics with each other. Again, this concept is not new. At nearly any diner in America, you can find a group of people sitting together discussing politics; but social media gives users the chance to forge a network larger than their local coffee shop. Unlike with the local network, social media users can simply ignore or "unfollow" opinions that do not match their own. Online networking allows people to find comfort in the crowd in the same way humans always have, but now on a much larger scale, with faster access to information.

Michigan State professor Anthony Olcott describes the wealth of information available on the internet as the "third information revolution," following the creation of writing and the invention of the printing press. Humans have always adapted to having access to more information, and, according to Olcott, homophily is just one method of countering the "indigestibility" of the large volume of information

available on the internet.[7] The problem of volume is just one of the challenges he calls the "The Six Vs" (Table 1).

Table 1. Challenge of the Six Vs

Volume	Massive amounts of information now produced and available on the internet.
Velocity	Information available in near real-time
Vector	Information no longer flows "downward, from authorities and elites to masses."
Veracity	Information may or may not be accurate
Verifiability	Source of information is difficult to prove
Vulgarity	From the Latin word "Vulgar," meaning from ordinary people.

Source: *Institutions and Information: The Challenge of the Six Vs,* Olcott

Each of Olcott's "Vs" challenge governments and institutions, even without the introduction of propaganda. On the other hand, the challenges presented to institutions by the Six Vs are likely beneficial for those who seek to exploit social media for propaganda because people online are already in a position to believe the same thing as the rest of their network; one is less likely to question information when it is already accepted by like-minded associates.

If social media facilitates self-reinforicng networks of like-minded users, how can a propaganda message transverse across networks? Consider the two networks in Figure 1. There are no overlapping nodes. While that may be the case with political beliefs, there may be connectors

[7] Anthony Olcott, "Institutions and Information: The Challenge of the Six Vs." ISD Working Paper in New Diplomacy. Institute for the Study of Diplomacy, Georgetown University, 2010.

on social media that fall within someone's interests, but outside of his or her political network. For example, a person may be a staunch Republican, but have social media connections with equally staunch Democrats because of their mutual interests in the same sports team.

However, this link between networks is only based on that single topic and can be easily severed. When it comes to politics in particular, people will sometimes not only reject the message coming from a particular user but will also reject that person as well. This dismissal on social media results in an "unfriending," or unfollowing of that user despite the connection made at some other level—just ask any social media users who cut ties with family members on social media during the 2016 election.

So, a loose and easily breakable connection is unlikely to impact large swaths of the population, which means that a "structural hole" exists between networks impeding flows of information between two opposing clusters of homophilic viewpoints.[8] Thus, to effectively employ social media to as a tool of propaganda, an adversary cannot rely on individual weak links between networks. Instead, an adversary can exploit a feature within the social media platform that enables cross-network data sharing on a massive scale: the trending topics list.

Trending topics are available on several different social media platforms, including the two most popular in the United States: Facebook and Twitter. Trends are visible to everyone. Regardless of who follows whom on a given social media platform, all users see the topics algorithmically generated by the platform as being the most popular topics at that particular moment. Given this universal and unavoidable visibility, "popular topics contribute to the collective awareness of what is trending and at times can also affect the public agenda of the

[8] Kadusin, 30.

community."[9] In this manner, a trending topic can bridge the gap between clusters of social networks. And further, a malicious actor can quickly spread propaganda by injecting a narrative onto the trend list.

Social Media Terminology

Before discussing propaganda in more depth, it is worthwhile to clarify some key concepts associated with social media. To start, we have the trend. As described above, a trending topic transcends networks and becomes the mechanism for the spread of information across social clusters. Several social media platforms provide a trends list. This paper focuses primarily on Twitter, a "microblogging" site where each post, called a "tweet," is limited to 140 characters.[10] Facebook also has a trends list, but it is less visible than the Twitter trends list; and the two applications serve different purposes.

Facebook dethroned MySpace as the most popular social media site around 2009, but it still maintains a similar function as MySpace, that of bringing friends and families together. Facebook, along with applications like Instagram and Snapchat, are like modern day postcards; you can share what you are doing and how you are feeling with an audience of followers. On Facebook, your connections are typically more intimate connections than you would expect on Twitter, which focuses less on bringing people together and more on bringing ideas together.

As a microblog, the core notion behind Twitter is to share your thoughts and feelings about the world around you with a group of people who share similar interests. The individuals who follow each other may

[9] Sitaram Asur, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang. "Trends in Social Media: Persistence and Decay." (Cornell University, 2011), 1.
[10] "Blog" is short for "web log." A blog is a way to share your thoughts via the internet. A microblog is a blog with a character limit to the text.

not be friends but could be a team of like-minded academics, journalists, sports fans, or politicos. When a person tweets, that tweet can be viewed by anyone who follows that person, or anyone who searches for that topic using Twitter's search tool. Additionally, anyone can "retweet" someone else's tweet, which broadcasts the original tweet to a new audience. Twitter makes real-time idea and event sharing possible on a global scale.[11]

For example, someone who is interested in what people are talking about on Twitter regarding Tom Brady can do a search within the application to discover what the average person thinks, as well as what sports experts are saying about Brady. If one searches for discussion on Tom Brady during the Super Bowl, the user doing the search will receive much more information than if he were to do a search during the off-season. In fact, one would expect that if Tom Brady is in the Super Bowl, his name would probably be trending during the game as the total tweets mentioning his name would cross the trend threshold for everyone to see on Twitter—even those who are not watching the Super Bowl or have no interest in Tom Brady.

Another method for quick referencing on Twitter is by using a "hashtag." A hashtag uses the symbol '#' to create a clickable link for the word that follows. Using the example above, a Twitter user could post a thought on the game, perhaps, "Nice pass, Brady," and include the hashtag #SuperBowl within the tweet. The tweet would then be visible to anyone who clicked on the link #SuperBowl, along with all of the other tweets using the same hashtag.

Because Twitter is an idea-sharing platform, it is very popular for rapidly spreading information, especially amongst journalists and academics; however, malicious users have also taken to Twitter for the

[11] Rani Molla, "Social Studies: Twitter vs. Facebook." *Bloomberg Gadfly.* February 12, 2016.

same benefits in recent years. At one time, groups like Al-Qaida preferred creating websites, but now, "Twitter has emerged as the internet application most preferred by terrorists, even more popular than self-designed websites or Facebook."[12] Twitter makes it easy to spread a message to both supporters and foes outside of a particular network. Groups trying to disseminate a message as widely as possible can rely on the trend function to reach across multiple networks.

There are three methods for controlling what is trending on social media: trend distribution, trend hijacking, and trend creation. The first method, trend distribution is relatively easy and requires the least amount of resources. Trend distribution is simply applying a message to every trending topic. Using the example above, someone could tweet a picture of the president with a message in the form of a meme—a stylistic device that applies culturally relevant humor to a photo or video—along with the unrelated hashtags #Brady and #SuperBowl. Anyone who clicks on those trends on the trend list expecting to see something about football will see that meme of the president. The other two methods of commanding the trend, trend hijacking and trend creation, require more resources in the form of either more followers spreading the message or a network of "bots" designed to spread the message automatically.

Bot Networks

Again, there are three methods of gaining command of the trend: trend distribution, trend hijacking, and trend creation. The latter, trend creation, requires the most effort. It necessitates money to promote a trend, knowledge of the social media environment, and a network of several automatic "bot" accounts.

[12] Weimann, 138.

Bot accounts are non-human accounts that automatically tweet and retweet based on a set of programmed rules. In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users, and now tops 15 percent.[13] Some of the accounts are "news bots," which just retweet the trending topics. Some of the accounts are for advertising purposes, which try to dominate conversations to generate revenue through clicks on links. Some bots are trolls, which, like a human version of an online troll, tweet to disrupt the civil conversation.

Of course, many groups – not just with malicious intent -- can benefit from trending topics on social media. Advertising firms routinely purchase trending topics, which Twitter marks with a "Promoted" tag. For seamless advertising, a company prefers "product placement" messages, which are similar in nature to a product placement in a television show.[14] The social media equivalent is called viral marketing, which employs seemingly non-affiliated social media accounts that tweet positive remarks about a particular brand.[15]

Vice News Tonight recently traveled to a marketing firm in London to cover a group of employees whose only discernable job skills were being young and understanding the social media environment. Those employees used their personal Twitter accounts to launch nation-wide advertising campaigns. During the interview, the marketing team decided to start a hashtag to promote a product. Within four minutes, their hashtag was trending across the whole of the UK.[16]

For malicious actors seeking to influence a population through trends on social media, the best way to establish trends is to build a

---

[13] Alex Lubben, "Twitter's users are 15 percent robot, but that's not necessarily a bad thing." VICE News. Mar 12, 2017.
[14] According to Jacques Ellul, advertising is the most effective form of propaganda because it places a message in the context of daily life.
[15] Kadushin, 10.
[16] Hind Hassan, "For millennials, by millennials: Startup Social Chain is taking social-media marketing to a new level." Vice.com, February 26, 2015.

network. The easiest way to build a network is to create bot accounts programmed to tweet at various intervals, respond to certain words, or retweet when directed by a master account. Figure 3 illustrates the basics of a bot network. The top of the chain is a small core group. That team is comprised of human-controlled accounts with a large number of followers. The accounts are typically adversary cyber warriors or true believers with a large following. Under the core group is the bot network. Bots tend to follow each other and the core group. Below the bot network is a group consisting of the true believers without a large following. These human-controlled accounts are a part of the network, but they appear to be outsiders because of the weaker links between the accounts. The bottom group lacks a large following, but they do follow the core group, sometimes follow bot accounts, and seldom follow each other.

Enough bots working together can quickly start a trend or take over a trend, but bot accounts themselves can only bridge the structural hole between networks, not completely change a narrative. To change a narrative, to conduct an effective influence operation, requires that a group combine a well-coordinated bot campaign with essential elements of propaganda.

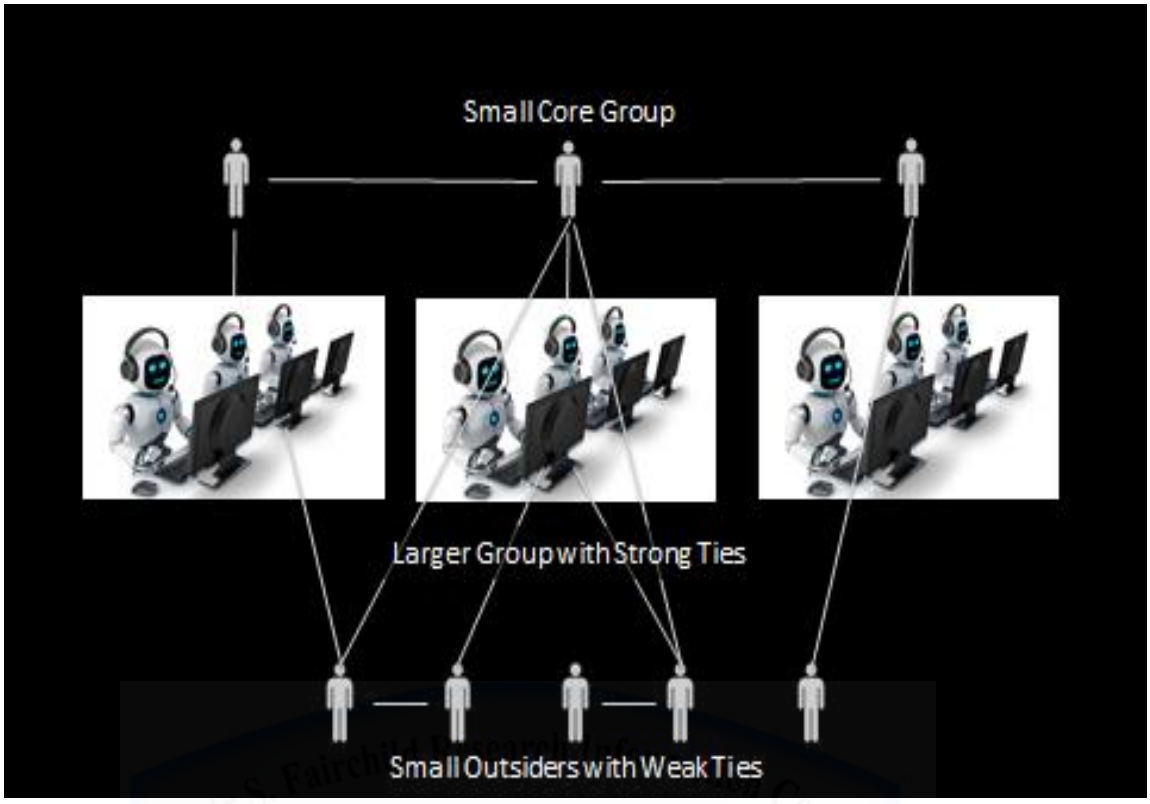


Figure 3. Illustration of a bot network
Source: Author

Propaganda Primer

Messaging designed to influence behavior has been around for centuries but became easier as methods of mass communication enabled wider dissemination of propaganda. During World War II, public service announcements (PSA) over the radio and on artistic posters connected a United States Government (USG) message directly to the American public. This form of propaganda helped recruiting, instilled patriotism, and encouraged behavior such as investing in war bonds or living within the limits of rationing. There are two kinds of propaganda employed by governments: propaganda to promote conformity amongst a domestic audience and information warfare designed to target a foreign audience.

The Cold War was somewhat of a high point for the research of propaganda because, according to a United States Information Agency (USIA) official in the early 1960s, "unless there is a suicidal nuclear war, the balance of power between ourselves [sic] and the communists will largely be influenced by public opinion."[17] The United States and the Soviet Union both took advantage of mass communications enabling the rapid spread of information as more people around the world started receiving news and information via television.

Observing the rise of mass media and its presence in daily life, French philosopher Jacques Ellul noted the simplicity of propaganda in 1965. According to Ellul, "Propaganda ceases where simple dialogue begins."[18] Essentially, propaganda permeates everyday experiences, and the individual targeted with a massive media blitz will never fully understand that the ideas he has are not entirely his own, just as researchers cannot fully determine the effectiveness of propaganda.[19]

Ellul also describes shared emotions within propaganda in the same way advertisers target mass-marketing campaigns: effective messaging targets an individual by providing a message to the masses, from which an individual could subsequently infer the masses all agree with the message.[20] This feeling of comradery provides legitimacy to both the emotion experienced and the message that brought about the particular feeling. A modern example of this phenomenon was observable during the Arab Spring as propaganda spread on Facebook "helped

---

[17] Phillip M. Taylor, *Munitions of the Mind: A History of Propaganda.* (Manchester University Press, 1995), 265.
[18] Jacques Ellul, *Propaganda: The Formation of Men's Attitudes.* (New York: Knopf, 1965), 6.
[19] Ellul, 11
[20] Ellul, 91.

middle-class Egyptians understand that they were not alone in their frustration."[21]

In short, existing emotions and beliefs are easier to exploit than beliefs that fall outside of an individual's social norms. Additionally, propaganda is simpler to grasp if everyone around a person seems to share the same emotions on a particular subject. Even a general discussion amongst the crowd can provide the illusion that propaganda is information.[22] In other words, propaganda creates heuristics, which is a way that the mind simplifies problem-solving by relying on quickly accessible data. Daniel Kahneman addresses the topic of heuristics and biases in his book, *Thinking, Fast and Slow*. One of the biases Kahneman describes is the concept that "what you see is all there is," or WYSIATI, for short. WYSIATI facilitates the achievement of coherence and cognitive ease that causes us to accept a statement as true.[23] Ingesting propaganda repeatedly is likely to make a person believe that WYSIATI.

Along with WYSIATI, Kahneman also addresses the recency bias or the "availability heuristic." Like WYSIATI, the availability heuristic weighs the amount and frequency of information received, as well as the recency of the information as more informative factors than the source or accuracy of the information. Essentially, the mind creates a shortcut based on the most—or most recent—information available, simply because it can be remembered easily. Often, the availability heuristic manifests itself in information received through media coverage. Understanding WYSIATI and the availability heuristic is important to understanding individual opinion formation (Figure 4), and how propaganda can exploit the shortcuts our minds make to form opinions.

---

[21] Thomas Rid, *Cyber War Will Not Take Place*. (New York: Oxford University Press, 2013), 132.
[22] Ellul, 85.
[23] Daniel Kahneman, *Thinking, Fast and Slow*. (New York: Farrar, Straus and Giroux, 2011), 87.

The lines in Figure 3 show formation of opinions temporally, with double arrows influencing a final opinion more than single arrows. The containers with red circles indicate a penetration point for propaganda exploitation. As previously described, mass media enables rapid spread of propaganda, which, in turn, feeds WYSIATI and the availability heuristic. The internet makes it possible to flood the average person's daily intake of information, which aids the spread of propaganda.

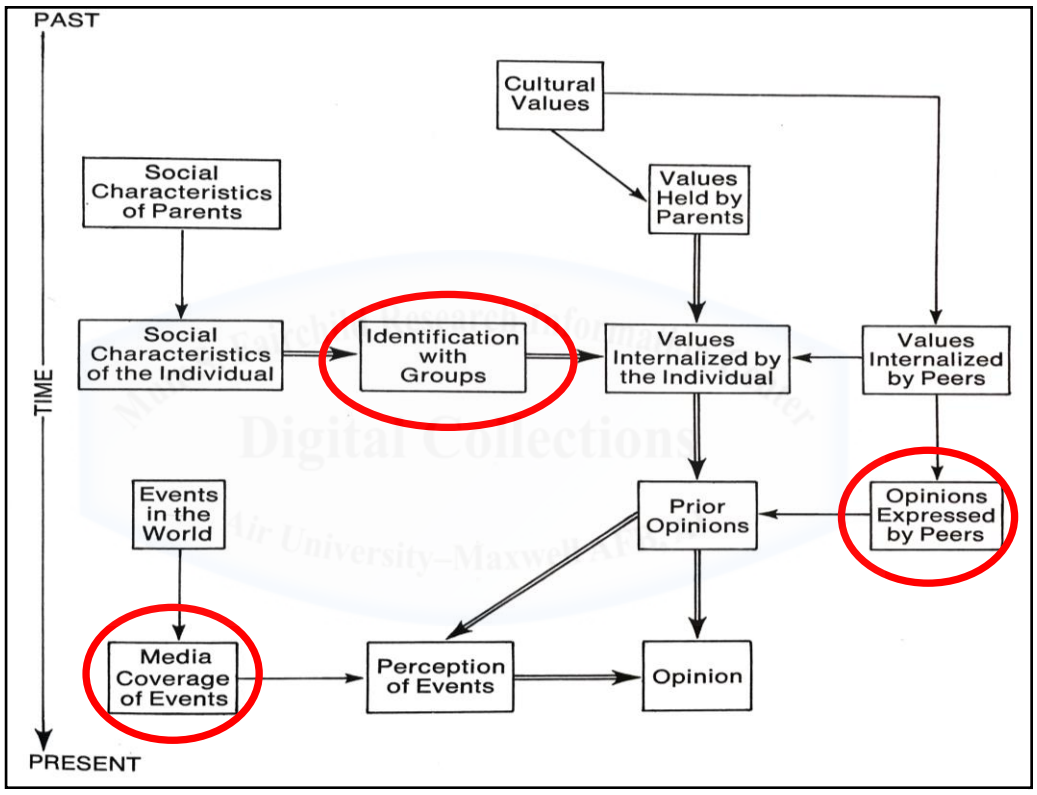


Figure 4. Model of individual opinion formation
Source: *Public Opinion in America*, Monroe, p. 147

Slobodan Milošević of Serbia was the first leader to make use of the internet combined with traditional media to spread the propaganda of his nationalist message. Milošević created a false story consisting of a modicum of historical truth in an attempt to re-write the history of Kosovo. Once he inserted his message into state-run media, it constantly circulated on radio, television, and via a newly established small e-mail network. Serbs slowly began to believe the propaganda because the new

history seemed similar enough to prior rumors to be believable. Additionally, it appeared that others shared the same emotions; and the repetition of the message created an availability heuristic for ethnic Serbs. The result was a human rights catastrophe as soldiers overcame "psychosocial dissonance created by this virtual reality" to commit genocide against their fellow citizens as they believed they were "saving Europe, even if Europe does not appreciate [their] efforts."[24]

Before the internet, technical limitations and high costs meant that governments once controlled most of the information that the public received.[25] In the case of Kosovo, the government used electronic media and traditional media to change the thoughts and opinions of the masses. Now, anyone with enough followers or bot accounts can disseminate a message to a broad audience via command of the trend.

Command of the trend enables the contemporary propaganda model, a "firehose of information" that permits the insertion of false narratives over time.[26] Because untruths can spread so quickly now, the internet has created "both deliberate and unwitting propaganda" since the early 1990s through the proliferation of rumors passed as legitimate news.[27] The normalization of these types of rumors over time, combined with the rapidity and volume of new false narratives over social media, opened the door for "fake news." It is also worth noting that the rise of social media came along with increases in computing power and mobile technology. In the early days of the internet, few people had an expensive computer with dial-up internet access in their homes. Now, most people have high-speed internet available on their mobile phones. As such, a firehose of false information is available at all times.

---

[24] Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era.* (Stanford, Calif.: Stanford University Press, 1999), 41.
[25] Olcott, 1.
[26] Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It." (Santa Monica, CA: RAND Corporation, 2016), 4.
[27] Jowett and O'Donnell, 159.

The availability heuristic and the firehose of disinformation can slowly alter opinions as propaganda crosses networks by way of the trend, but the amount of influence will likely be minimal unless it comes from a source that a non-believer finds trustworthy. An individual may see the propaganda and believe the message is popular because it is trending, but still not buy into the message itself. Instead, the individual will likely turn to a trusted source of news to test the validity of the propaganda. Therefore, we must now analyze modern journalism to determine how command of the trend can transform propaganda from fake news to real news.

Modern Journalism

Social media has changed the news landscape exactly as Rupert Murdoch predicted. The evidence of online journalism is on display at The Newseum in Washington DC, where tourists gather outside every day to observe the front pages of newspapers from every state prominently on display in front of the building. The papers seem like relics of days gone by, as people snap photos of the case of newspapers using the device by which more and more Americans receive their news: the mobile phone.

Currently, 72% of Americans get digital news primarily from a mobile device, and people now prefer online news sources to print sources by a ratio of 2:1.[28] The news consumer now selects from an abundance of options besides a local newspaper, based on how the consumer perceives the credibility of the resource. Along the lines of social networking and propaganda, people are more willing to believe things that fit into their worldview. Once source credibility is established,

[28] Katerina Eva Matsa and Kristine Lu. "10 facts about the changing digital news landscape." Pew Research Center. September 14, 2016.

there is a tendency to accept that source as an expert on other issues as well, even if the issue is unrelated to the area of originally perceived expertise.[29]

The combination of networking on social media, propaganda, and reliance on unverifiable online news sources introduces the possibility of completely falsified news stories entering the mainstream of public consciousness. This phenomenon, commonly called fake news, has generated significant criticism from both sides of the American political spectrum, with some labeling any contrary viewpoints fake. In reality, fake news consists of more than just bad headlines, buried ledes, or poorly sourced stories.[30] Fake news is a particular form of propaganda comprised of a false story disguised as news. On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news stories.

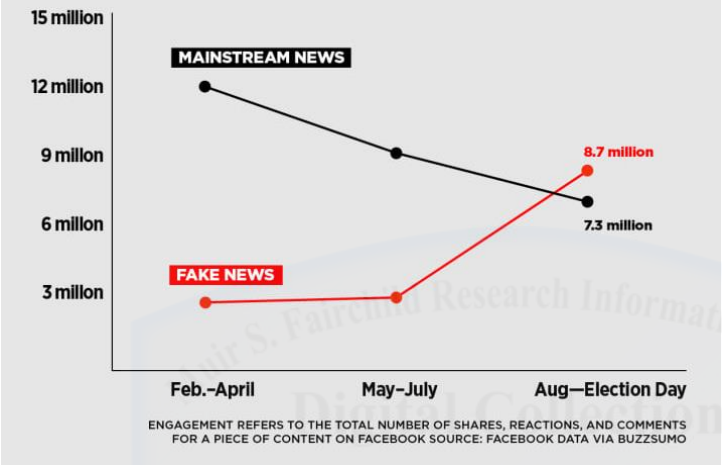


Figure 5. Total Facebook engagements for top 20 election stories
Source: Craig Silverman, Buzzfeed News

A prime example of fake news and social media came from the most shared news stories on Facebook during the 2016 US presidential election. The source of the fake news was a supposedly patriotic American news blog called "End the Fed," a website run by Romanian businessperson Ovidiu Drobota. One story stating that the Pope

[29]Jowett and O'Donnell, 300.
[30] According to Merriam-Webster.com, "in journalism, the lede refers to the introductory section of a news story that is intended to entice the reader to read the full story. It appears most frequently in the idiom 'bury the lede.'"

endorsed Donald Trump for President received over one million shares on Facebook alone, not to mention shares on Twitter.[31] Other fake news stories from that site and others received more shares in late-2016 than traditional mainstream news sources (see Figure 5).[32]

It is important to recognize that more people were exposed to those fake news stories than what is reflected in the "shares" data. In some cases, people would just see the story in a Facebook or Twitter feed; in many cases, people actively sought out news from those sources, which are fiction at best, foreign propaganda at worst. Over time, those fake news sources become trusted sources for some people. As people learn to trust those sources, legitimate news outlets become less trustworthy.

At one time, the American public had confidence in the news media; a 1975 Roper Organization survey found the majority of respondents thought the institution was trustworthy and unbiased, with only 7 percent of everyone polled feeling that the media leaned too far to the political left, and only 2 percent felt it leaned too far to the right.[33] Conversely, a 2016 poll by Gallup showed American trust in mass media is at an all-time low.[34]

Olcott's Six Vs are relevant to modern journalism, particularly velocity, volume, and vector. When news is tailorable to one's taste, and new stories are popping up around the world every second, mainstream journalists have to change their methods to compete with other sources of news. Therefore, if social media is becoming a source for spreading news and information, journalists must keep up by using social media to spread their stories and to acquire information in the first place.

---

[31] Tess Townsend, "Meet the Romanian Trump Fan Behind a Major Fake News Site." Inc.com, November 21, 2016.
[32] Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook." Buzzfeed News. November 16, 2016.
[33]Alan D. Monroe, *Public Opinion in America.* (New York: Dodd, Mead, 1975), 121.
[34] Art Swift, "Americans' Trust in Mass Media Sinks to New Low." *Gallup*, September 14, 2016.

According to an Indiana University School of Journalism study, the most common use of social media for journalists is to check for breaking news.[35] One reporter emphasized, "Everybody in the media is on Twitter. It is the place where news breaks the fastest. When something is going on in the market, I don't Google it — I go on Twitter."[36] As a result, mainstream journalists tend to use tweets as a legitimate source, especially when there is a lack of more valid or confirmed sources.[37] Overreliance on social media for breaking news can become problematic in the midst of an ongoing information operation. If an adversary can take control of a trend on Twitter, the trend is likely to be noticed by mainstream media journalists. Even more problematic, the mainstream media may provide legitimacy to a false story by covering the topic—essentially turning fake news into real news.

Weaponizing Social Media

Web 2.0 laid the foundation for the weaponization of social media via increased computing power, mobile technology, and the increasing use of social media as a news source. To summarize, social media was originally intended to bring people together to share thoughts and ideas. Around the time social media rose in popularity, news content was continuing to move from print and television to online sources. The two ideas converged when News Corp bought MySpace in 2005, providing more control for consumers of news, and essentially allowing them to become producers of news. Group dynamics are unchanged with social media, which enables people to hear ideas they agree with instantly and

[35] Andrea Peterson, "Three charts that explain how U.S. journalists use social media." *The Washington Post.* May 06, 2014.
[36] Matt Pressberg, "Why Even Donald Trump Can't Save Twitter." TheWrap.com. March 21, 2017.
[37] Weimann, 138.

whenever they choose; and they can feel comfortable knowing that they are not alone in their thoughts. This is the initial setup for how social media became weaponized via an adversary's propaganda.

One of the primary principles of propaganda is that the message must resonate with the target. Therefore, when presented with information that is within your belief structure, your bias is confirmed, and you accept the propaganda. If it is outside of your network, you may initially reject the story, but the volume of information may create an availability heuristic in your mind. Over time, propaganda becomes normalized, and even believable when the massive amount of information—even if it is disinformation through fake news—starts to seem like "what you see is all there is" (WYSIATI). WYSIATI is confirmed when a fake news story is reported by the mainstream media, which has become reliant on social media for spreading and receiving news.

Figure 6 maps the process of how propaganda can penetrate a network that is not predisposed to the message. This outside network is a group that is ideologically opposed to the group of true believers. The outside network is likely aware of the existing narrative but does not necessarily subscribe to the underlying beliefs that support the narrative. The mechanism for an adversary to spread propaganda is the social media trend. A synchronized network of true believers and bot accounts can create or hijack a trend. Trending items produce the illusion of reality; in some cases even being reported by journalists.

The next two chapters are case studies of how ISIS and Russia successfully manipulated social media, particularly Twitter. Although the subjects of the case studies had different objectives, the tools and techniques were similar. Foreign actors in both cases utilized four essential elements on social media -- propaganda narratives, true believers, cyber warriors, and a bot network -- to spread propaganda that influenced the emotions, opinions, and behavior of US citizens in a

manner antithetical to US interests. In short, ISIS and Russia weaponized social media via command of the trend.

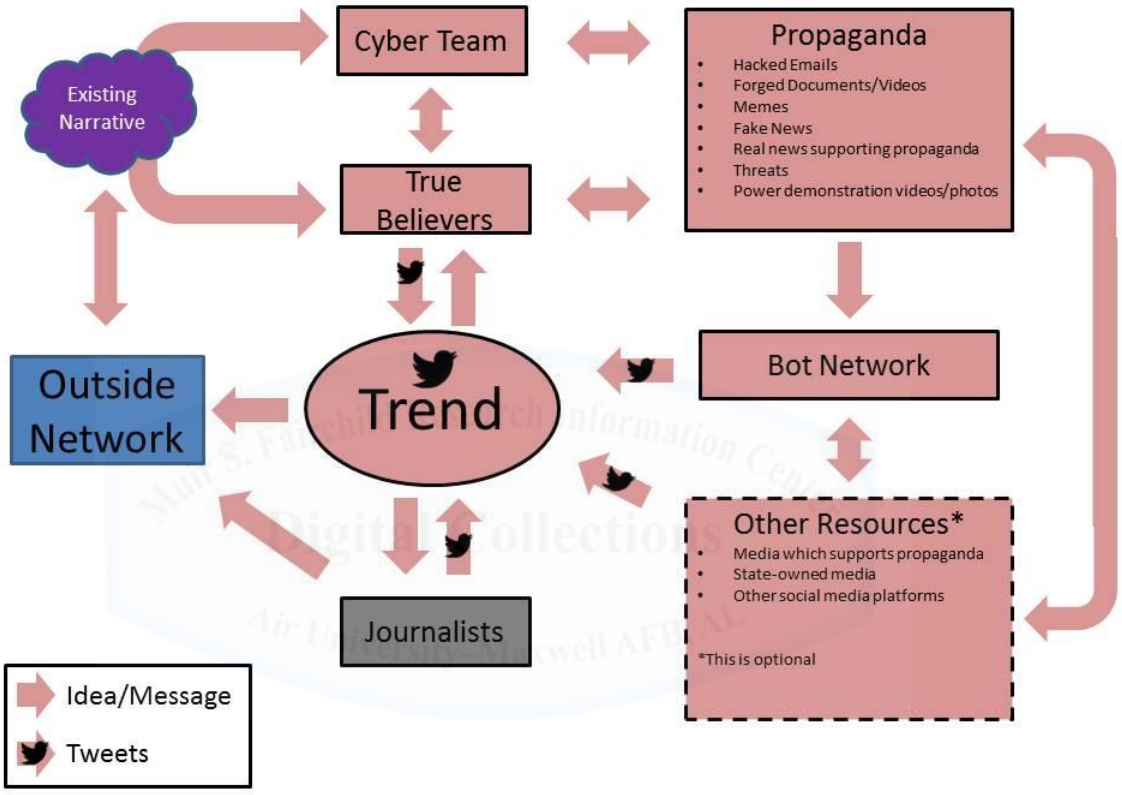


Figure 6. Process map of how propaganda spreads via the Trend
Source: Author

Chapter 2

ISIS: The Genesis of Social Media Weaponization

> *ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.*
>
> FBI Director James Comey, 2015

ISIS is either a large terrorist organization or a very fragile state with a weak army. In reality, it seems to be more of the latter when compared to earlier terrorist organizations; however, the perception of ISIS varies depending on the source. ISIS is a religious caliphate to believers in the teachings of the group leader, al-Baghdadi. Much of the rest of the world assumes that ISIS is a terrorist group that represents a perversion of faith. That viewpoint fails to understand the intent of ISIS and drastically underestimates the group. As the Commander of US Special Operations Command (USSOCOM), Major General Michael Nagata suggested, "We have not defeated the idea" because "…we do not even understand the idea."[1]

The lack of understanding of ISIS branding was a contributing factor for the failure of the United States, and the international community, to establish an effective counter-messaging strategy for ISIS' presence on social media. The propaganda produced by the State Department, for example, clearly did not resonate with the target

[1] Graeme Wood, "What ISIS Really Wants." *The Atlantic*. March 2015.

audience. This failure to communicate was mainly because the audience was never truly defined, and the message was not central to anyone's worldview.

ISIS, on the other hand, managed to master the art of manipulation because a single message simultaneously targeted potential allies and foes alike. ISIS' use of social media is a case study in effective propaganda techniques that bolstered recruiting, increased brand recognition, and spread terror with minimal effort. ISIS quickly became the first organization to weaponize social media effectively. This chapter analyzes the organization and its use of social media to achieve its goals.

ISIS Objectives

The biggest misconception when observing ISIS at a superficial level is to assume that ISIS is a terrorist organization. Although ISIS may use terrorism as a tactic, the organization behaves differently than any other terrorist organization in the world.[2] The differences are apparent in every aspect from operations, to recruiting, to governing. The last factor is the key discriminator: terrorist groups terrorize, they do not govern. As a descendant of al-Qaeda in Iraq, the group struggled to find its way after the death of al-Zarqawi in 2006; under the leadership of al-Baghdadi the group has established clear lines of authority, taxation and educational systems, trade markets, even policing and a judiciary (covering civil, criminal, and religious complaints).[3] Gaining and holding land is just a part of what ISIS believes is the destiny of the organization and its

[2] Audrey Kurth Cronin, "ISIS Is Not a Terrorist Group" *Foreign Policy.* March/April 2015.
[3] Stephen M. Walt, "ISIS as Revolutionary State." *Foreign Policy,* November/December 2015, 42

followers. Certainly, the desire is to create a Caliphate,[4] but its ultimate purpose is more apocalyptic in nature: ISIS seeks to usher in the end of the world.[5] ISIS members believe that their actions will bring the forces of the world to attack their Caliphate and result in the imminent defeat of the Islamic army in the Syrian town of Dabiq, thus triggering the end of the world and the final purge of evil.[6] ISIS is a revolutionary force with doomsday cult beliefs.[7]

To advance the organization's objectives, ISIS used one single message that served to spread its propaganda on social media to a broad audience that fit within a narrative of strength for the supporter, and a narrative of terror for the adversary. In other words, ISIS cyber warriors combined propaganda with command of the trend to accomplish three things with one message. First, they demonstrated the weakness and incompetence of the international community to fight them online and on the battlefield. Secondly, they injected terror into the mainstream media. Finally, and most importantly, they recruited new fighters to join them on the battlefield in Iraq and Syria—and online.

How ISIS Dominated Social Media

Through a combination of slick marketing and cyber mastery, ISIS bolstered its message around the world. The first thing that the group refined was the ISIS branding. The organization projects a very specific image to the world that affects the viewer differently based on beliefs. To a follower, the images that are shared via social media demonstrate

---

[4] Caliphate: "a form of Islamic government led by a—a person considered a political and religious successor to the Islamic prophet, Muhammad, and a leader of the entire Muslim community. Source: Kadi, Wadad and Shahin, Aram A. "Caliph, caliphate". *The Princeton Encyclopedia of Islamic Political Thought*, 2013: 81–86.
[5] Wood, 3
[6] Dabiq is also the name of the ISIS magazine, which is available electronically and spread via social media.
[7] Walt, 43

strength and power. To the non-follower, the images are grotesque and horrifying. In other words, no matter what ISIS puts out in social media the result is a win for the organization because the same message successfully targets two different groups. The amplification of those messages by creating trends on Twitter is guaranteed to get further attention once the tweet falls into the mainstream media. Thus, ISIS is capable of using relatively small numbers of Twitter users (see Table 2, below) to project an aura of strength.

The method for expanding the reach of a single ISIS tweet or hashtag involves a network of legitimate retweets combined with bots and unwitting Twitter users. While ISIS does maintain a strong network of true believers, the numbers are relatively small and spread thinly across the Middle East. Therefore, ISIS must game the system and rig Twitter for a message to go viral. One high-tech method for creating a bot network was a mobile app called "Dawn of Glad Tidings." The app, designed by ISIS cyber warriors, provides updates on ISIS activities and spiritual guidance to the user. When users download the app, they create an account that links to their Twitter account, which then gives the app generous permissions allowing the app to tweet using that user's account.[8] The app then retweets on behalf of the user when a master account sends an ISIS-branded tweet.

Over time, the hashtag generates enough tweets to start localized trends. Once the trend surfaces, it is broadcast over trend-monitoring networks, like the Arabic Twitter account, @ActiveHashtags.[9] That causes the hashtag to gather more attention across the region, and then be retweeted by real followers and other bot accounts. The final step in the process is when the trend goes global.

[8] Berger, "How ISIS Games Twitter"
[9] Berger, "How ISIS Games Twitter"

Table 2. Snapshot of ISIS Twitter Activity

Estimated number of overt ISIS Twitter accounts	46,000
Number of "bot" accounts	6,216
Avg number of tweets per day per user	7.3
Avg number of followers	1,004
Most common year accounts created	2014
Top Languages	Arabic (73%), English (18%), French (6%)
Top Locations	"Islamic State," Syria, Iraq, Saudi Arabia*

Source: "The ISIS Twitter Census" Brookings Institute, March 20, 2015.
* Based on location-enabled users and self-defined account locations

Worldwide trends on Twitter have been a boon for ISIS. Creating and hijacking trends garnered attention for the group that would otherwise have gone unnoticed on social media. The peak of ISIS trend hijacking was during the World Cup in 2014. As one of the world's most popular sporting events, it was no surprise that the hashtag #WorldCup2014 trended globally on Twitter non-stop during the tournament. At one point though, nearly every tweet under this hashtag had something to do with ISIS instead of soccer. The network of ISIS supporters and bot accounts hijacked the trend. Because people were using the hashtag to discuss the matches, and advertisers were using the trend for marketing, Twitter struggled to stop the trend and the subsequent ISIS propaganda effort.

In fact, ISIS cyber warriors and true believers foiled most of the early attempts by Twitter to stop ISIS from using their platform to spread propaganda. Twitter's initial reaction was to suspend accounts that violated the user terms of the agreement. The result was creative user names by ISIS supporters; for example, a user named @jihadISIS42 was

created after @jihadISIS41 was suspended, which was set up after @jihadISIS40 was suspended.[10] Each new account demonstrated a deep dedication to the cause that, when combined with the seemingly significant presence on social media, presented the group as dominating social media.

In the case of #WorldCup2014, ISIS took command of the trend by hijacking, using the opportunity to push recruiting messages, and make terror threats against the tournament venues in Brazil. Additionally, the co-opted hashtag often directed users to other hashtags in what was ultimately a successful attempt to generate worldwide trends of other ISIS related themes. One successful hashtag-creation effort was #StevensHeadinObamasHands, which included memes of President Obama and ISIS-held American journalist Steven Sotloff (example in Figure 5). The implication was that the President of the United States did not care to or was powerless to stop the murder of an American citizen. Once again, ISIS appeared to be disproportionately powerful because of the command of the trend.

Figure 7. ISIS hashtag creation, 2014
Source: Screenshot, unknown user, Twitter.com

Due to the organization's aggressive communications strategy and branding, the ISIS social media presence consistently

[10] "Terrorist Use of Social Media: Policy and Legal Challenges" DC Roundtable Forum. Council on Foreign Relations. October 14, 2015.

outperforms similar jihadist groups in the region that have the same number of, or more, followers.[11] Unlike al-Qaeda, which largely limited its online activity to websites, ISIS wants to communicate with a broader audience—it wants to communicate directly to the whole world. In addition to spreading terror threats, the appearance of the group as a powerful state appealed to a group of true believers who turned to the group as new recruits to the fight in Iraq and Syria.

The Recruits

Years of research and profiling to determine an accurate demographic for radicalization have resulted in "few consistent patterns and no reliable profile."[12] Terrorist groups like al-Qaeda historically targeted religiously passionate and disenfranchised Middle Eastern young men. ISIS, on the other hand, recruits worldwide from both sexes and every age and level of religiosity. While there may not be specific demographics, there are essentially three motivations for recruits: religion, fear, and adventure, each of which can be advertised using appealing videos and photos spread on social media.[13]

ISIS' objectives make the group particularly appealing to those who desire increased piety. One oddity in ISIS recruiting is the slaughter of fellow Muslims. Al-Qaeda sought to recruit fervently religious men; hence, they carefully avoided harming fellow Muslims to prevent offending devout pledges. Ironically, ISIS is "impervious to the risk of backlash" from killing Muslims; in fact, the caliphate bolsters its image and gets recruiting bumps with nearly every execution video.[14] These

[11] Berger, "How ISIS Games Twitter"
[12] J. M. Berger, "ISIS and the Foreign-Fighter Phenomenon." *The Atlantic*. March 8, 2015.
[13] Cronin, 3.
[14] Cronin, 3.

post-execution recruiting spikes imply two things. First, they are garnering support from those who genuinely believe that al-Baghdadi is the caliph. These true believers would interpret the murders as admissible killings for the crime of apostasy.[15] Second, ISIS gained support from those who fear ending up like the helpless souls horrifically murdered for lack of support or their perceived lack of holiness. Interviews with imprisoned ISIS members in Iraq revealed a common desire: security for themselves and their families. ISIS provided an outlet for them to fight for the dignity of themselves, their family, and their tribe.[16] In exchange, the fighter and family live without fear of accusation of being "apostates."[17] Once again, ISIS can use social media to spread fear in support of their objectives while using those same images to spark an interest among the true believers.

Most of the ISIS true believer recruits from the Middle East and abroad join for a variety of factors, including adventure and prestige. These notions are exploited by ISIS propaganda on social media. Erin Saltman, a researcher at the Institute for Strategic Dialog, summarized the vast majority of ISIS recruiting "plays upon the desires of adventure, activism, romance, power, belonging, along with spiritual fulfillment."[18] Evidence of this fantasy world is apparent in ISIS-produced recruiting videos, tweets, and even computer games (see Figure 8).

ISIS used social media from 2014-2016 to demonstrate power, sow fear in the international audience, and recruit the true believers. All the while, they used the true believers following on social media to boost their trends on social media. However, the group currently finds itself altering its modus operandi due to the recent loss of territories in Iraq

---

[15] Apostasy is the abandonment of a particular religion. Some interpret Quarnic verses to read that the punishment for apostasy is death within Sharia Law.
[16] Lydia Wilson, "What I Discovered From Interviewing Imprisoned ISIS Fighters." The Nation. October 21, 2015.
[17] Wood, 10.
[18] Wood, 10.

Figure 8. Familiar Narratives: ISIS Video Game Propaganda
Source: "Networking in the Market for Loyalties," Sharma

and Syria, combined with a spate of successful terrorist-style attacks in Europe. The ongoing worry for counter-terrorism experts is finally beginning to come to fruition: the recruit staying home to fight, instead of joining ISIS overseas.

The Lone Wolf

After years of maintaining a significant presence on social media, ISIS is using Twitter less now for official communication. The reasoning is likely two-fold. First, the group has lost territory in Iraq and Syria and is adjusting their strategies. Secondly, Twitter has removed over 600,000 ISIS-related accounts consisting of bots, cyber warriors, and true believers.[19] Additionally, Twitter has adjusted the program to find terror-related videos, memes, and photos soon after an account from the ISIS network posts the propaganda. Adapting to the changes, ISIS started

[19] Carleton English, "Twitter continues to wage its own war against ISIS." *New York Post*, March 21, 2017.

using secure messaging tools like Telegram and WhatsApp. Messaging services like WhatsApp are not publicly visible; therefore, the ISIS message is not spread across networks the way it once was using Twitter to gain command of the trend. Instead, the organization can still spread a message rapidly across their network of cyber warriors and true believers using secure messaging tools, and it can be done with little risk of detection. In fact, one of ISIS' best-known recruiter's Twitter profile "instructed newcomers to contact him via the encrypted messaging app Telegram."[20] It is uncertain how this messaging will impact recruiting goals, but what is certain is that it allows ISIS recruiters to aid foreign fighters in planning attacks around the world. [21]

The added benefit of the "lone wolf" brand of terrorism recruits is that an attack can dominate the trends—and the headlines—albeit differently than trend hijacking or creation using a bot network. Media coverage of lone wolf attacks fans the flames, and the message still spreads by way of the trend. The more people talk about the event, the more the ISIS message spreads without the group creating propaganda. Presumably, this free advertising generated by an individual acting alone after pledging allegiance to ISIS has the same effect on the psyche of its victims and possible recruits as original social media campaigns from 2014-2016. The trend draws attention to the group, creates fear, and creates more recruits who then attempt to mimic the original lone wolf attack. The cycle repeats, and ISIS maintains a narrative of strength. In short, ISIS was able to do the same thing without attacks on foreign soil by taking command of the trend but now requires a lone wolf attack to create trends because of the diminished power of their cyber warrior and bot network.

---

[20] Rukmini Callimachi, "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar." *The New York Times.* March 5, 2007.
[21] Lizzie Dearden, "Khalid Masood: Suspected Isis supporter used WhatsApp two minutes before London attack." *The Independent.* March 24, 2017.

Summary

With ISIS seemingly dominating social media from 2014-2016, it is easy to fixate on that impression and assume that they won popular support. The fact is that ISIS only has a limited number of fighters, and its support around the world—even in Muslim countries—is minuscule (see Figure 7).[22] The fact that the group appeared so strong on social media is, quite simply, proof that command of the trend is an effective tool for amplifying voices and projecting power. One of the reasons ISIS seems so powerful is that when viewed through the lens of terrorist groups, the organization seems vast because terrorist groups do not have territory—ISIS does, and it advertises that fact using weaponized social media campaigns. Its slick social media presence, ghastly videos, massive recruiting, and victories against Iraqi security forces make ISIS seem disproportionately stronger than it is. The group overran Mosul with only a few thousand fighters, but the corresponding viral social media campaign implied a large force had just earned a massive victory.[23]

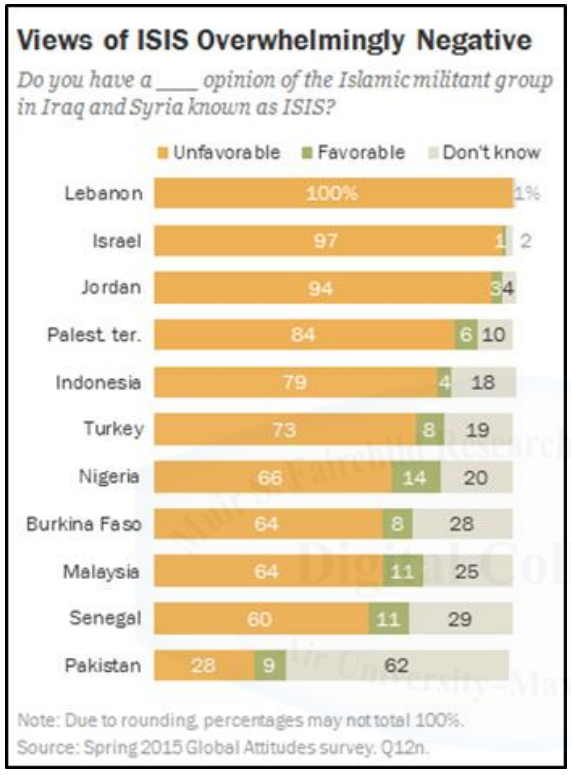


Figure 9. Muslim opinion of ISIS
Source: In Nations with Significant Muslim Populations, Much Disdain for ISIS," Pew Research.

[22] "In Nations with Significant Muslim Populations, Much Disdain for ISIS." Pew Research Center. November 17, 2015.
[23] Berger, "How ISIS Games Twitter."

In summation, ISIS serves as a model for any non-state group attempting to use social media for cyber warfare. Social media, specifically Twitter, made the organization appear to be more potent and highly regarded than it is, and it amplified the voices of supporters and potential recruits. Table 3 summarizes ISIS' use of the four requirements to gain command of the trend (propaganda narratives, true believers, cyber warriors, and a bot network) based on the analysis within this case study.

Table 3. ISIS Case Study Analysis

Propaganda Narratives	1. ISIS is strong; everyone else is weak. 2. True believers should join the cause.
True Believers	Muslims believing in the Caliphate of al-Baghdadi
Cyber Warriors	Propaganda makers, video editors, app programmers, recruiters, spiritual leaders using low and high-tech tools to advertise ISIS on Social media.
Bot Network	Unwitting victims of spiritual guidance app "Dawn of Glad Tidings."

Source: Author

At the same time ISIS was weaponizing Twitter, Russia was using it to simultaneously cause confusion and garner support for its invasion of Crimea; 2014 marked the beginning of influence operations in Europe, culminating in a massive disinformation campaign following the shoot-down of Malaysia Airlines Flight 17 in July. Soon, the command of the trend would be used by a state actor to target the United States—Russian involvement in the 2016 Presidential Election.

Chapter 3

Russia: Masters of Manipulation

I'm warning you: We are at the verge of having 'something' in the information arena, which will allow us to talk to the Americans as equals.

Senior Kremlin Advisor Andrey Krutskikh, 2016

Russia is no stranger to information warfare. During the Cold War, Soviet agents used "forgeries and press placements to disparage candidates" in the United States and around the world.[1] Nowhere was the Soviet campaign more noticeable than with the change of French attitudes because of a "slow penetration by propaganda." Throughout the 1950s, France noticed a dramatic shift of the political spectrum to the left, resulting in the election of communist and socialist candidates.[2]

The original technique of Soviet actors was through "*aktivnyye meropriyatiya*" (active measures) and "*dezinformatsiya*" (disinformation). According to a 1987 State Department Report on Soviet information warfare, "Active measures are distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/or publics."[3]

In other words, Soviet agents would try to weave propaganda into an existing narrative to smear countries or individual candidates. For

---

[1] ODNI Report, 5.
[2] Ellul, 288.
[3]United States Department of State, Report: *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87*, (Washington D.C.: Bureau of Public Affairs, 1987), viii.

example, the same report suggests that various rumors about the spread of AIDS during the 1980s were proliferated because of Soviet active measures. One narrative stated that the Department of Defense was responsible for the epidemic after creating the virus as a biological weapon.[4] The AIDS rumor was published in newspapers around the world based on studies from front organizations within academia, as well as using supposed experts to give speeches in universities and think tanks in the United States and Europe.

Active measures are designed, as retired KGB General Oleg Kalugin once explained,

> To drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs. The most common subcategory of active measures is dezinformatsiya, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister.[5]

The techniques that Russia uses today are similar to the Cold War, but the dissemination is more widespread through the weaponization of social media. Recently, the Russian Minister of Defense acknowledged the existence of their cyber warriors in a speech to the Russian Parliament, by announcing that Russia formed a new branch of the military consisting of information warfare troops.[6] Unlike non-state actors like ISIS trying to generate buzz on Twitter, Russia possesses both a history of spreading propaganda and an army of professional trolls whose mission is to fight online.

---

[4] S*oviet Influence Activities,* 34.
[5] Natasha Bertrand, "It looks like Russia hired internet trolls to pose as pro-Trump Americans." *Business Insider*, July 27, 2016.
[6] Vladimir Isachenkov, "Russia military acknowledges new branch: info warfare troops." AP News. February 22, 2017.

Unlike ISIS cyber warriors, the Russian trolls have a variety of state resources at their disposal, including a vast intelligence network to assist their cyber warriors. The additional tools available to Russia also include RT (Russia Today) and Sputnik, the Kremlin-financed television news networks broadcasting in multiple languages around the world. According to the Office of Director of National Intelligence (ODNI) Report on Russian Influence in the 2016 US Presidential Election, "Moscow's influence campaign followed a messaging strategy the blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state funded media, third-party intermediaries, and paid social media users, or 'trolls.'"[7]

Before the trolls begin their activities on social media, the cyber warrior hackers first provide hacked information to Wikileaks, which according to CIA director Mike Pompeo, is a "non-state hostile intelligence service abetted by state actors like Russia."[8] In intelligence terms, WikiLeaks operates as a "cutout" for Russian intelligence operations—a place to spread intelligence information through an outside organization—similar to the Soviets use of universities to publish propaganda studies in the 1980s.[9] The trolls then take command of the trend to spread the hacked information on Twitter, referencing WikiLeaks and links to RT news within their tweets.

These Russian efforts would be impossible without an existing network of American true believers willing to spread the message. In the case of the 2016 election, Russian propaganda easily meshed with right-wing networks known as the "alt-right" and the so-called "Bernie Bros," who lashed out on Twitter because Hillary Clinton beat Senator Bernie Sanders in the Democratic Party primary. The Russian trolls and the bot

---

[7] ODNI Report, "Key Judgements," ii.
[8] Richard Gonzalez, "CIA Director Pompeo Denounces WikiLeaks As 'Hostile Intelligence Service." *NPR*. April 23, 2017.
[9] Malcolm Nance, *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*. (Skyhorse Publishing. Kindle edition, 2016), 1,839.

accounts amplified the voices of the true believers in addition to inserting propaganda into that network. Then, the combined effects of Russian and American Twitter accounts took command of the trend to spread disinformation across networks.

Before 2016, Russian active measures were also used in European elections, most notably the "Brexit" campaign. One European expert on Russia quoted in *The Atlantic* article "War Goes Viral" summarized Putin's intent as, "not to make you love Putin," instead, "the aim is to make you disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate."[10] Active measures enable manipulation. Smearing political candidates, hacking, the spread of disinformation, and hoaxes all contribute to a breakdown of public trust in institutions.

Active Measures and Disinformation

On September 11, 2014, the small town of St. Mary Parish, Louisiana, was briefly thrown into a panic when residents began hearing reports through text, social media, and on local television stations that a nearby chemical plant fire was spreading toxic fumes that would soon endanger the whole town. A reasonable snap-judgement would imply the anniversary of 9/11 meant the fire was likely an act of terrorism and the casualties would be high. However, the tragedy of this story is not the loss of life; it is that the panic was based on a hoax. The entire narrative was based on falsified—but very real looking—online news stories, hashtag manipulation, and mass-texts (SMS) to various numbers with the local area code and dialing prefix. The story developed so quickly and was so sensational that local news outlets had no choice but to cover the

[10] Robinson Meyer, "War Goes Viral: How Social Media is Being Weaponized Across the World." *The Atlantic*. October 18, 2016.

situation as soon as possible. The actual source for the news was not the chemical factory; it was a nondescript building in St. Petersburg, Russia, where an army of online cyber-warrior trolls seeks to distribute false information.[11]

The Internet Research Agency, as it was called in 2015, now seems to be the information warfare branch openly admitted by the Russian Minister of Defense. The cyber trolls produced several hoaxes in the United States and Europe, like the Louisiana hoax, according to Adrian Chen in his article "The Agency" in *The New York Times Magazine*. Protests of police departments throughout the United States during the summer of 2015 provided several opportunities to manipulate narratives via social media, and it is likely that Russian trolls hijacked some of the Black Lives Matter related trends to spread disinformation and accusing journalists of failing to cover important issues.[12] The Russian trolls said that the idea was to spread fear, discrediting institutions—especially American media—while making President Obama look powerless and Putin more favorable.[13]

Several hijacked hashtags in 2015 attempted to discredit the Obama administration while spreading racist memes and hoaxes aimed at the African-American community. In other words, the Russian trolls seemed to target multiple groups to generate anger and create chaos. One particularly effective Twitter hoax occurred as racial unrest fell on a university campus that fall.

#PrayforMizzou

---

[11] Adrain Chen, "The Agency." *New York Times Magazine*, June 2, 2015.
[12] Senate Intelligence Committee Testimony, "Disinformation: A Primer In Russian Active Measures And Influence Campaigns" Clint Watts, March 30, 2017.
[13] Chen, "The Agency."

On the night of November 11, #PrayforMizzou began trending on Twitter. [14] The trend was a result of protests at the University of Missouri campus over racial issues; however, "news" slowly started developing within the hashtag that altered the meaning, and soon shot the hashtag to the top of the trend list. The news was that the KKK was marching through Columbia and the Mizzou campus. One user, display name, "Jermaine" (@Fanfan1911), warned residents "The cops are marching with the KKK! They beat up my little brother! Watch out!" Jermaine's tweet included a picture of a black child with a severely bruised face; it was retweeted hundreds of times. Additionally, Jermaine and a handful of other users continued tweeting and retweeting images and stories of KKK and neo-Nazis in Columbia, chastising the media for not covering the racists creating havoc on campus.

Looking at Jermaine's followers, and the followers of his followers, one could observe that the original tweeters all followed and retweeted each other. Those users also seemed to be retweeted automatically by approximately 70 bots. These bots also used the trend distribution technique, which used all of the trending hashtags at that time within their tweets, not just #PrayforMizzou. Spaced evenly, and with retweets of real people who were observing the Mizzou hashtag, the numbers quickly escalated to thousands of tweets within a few minutes. The plot was smoothly executed and evaded the algorithms Twitter designed to catch bot tweeting, mainly because the Mizzou hashtag was being used

[14] Because of the Adrian Chen article, I observed particular tweeting patterns of certain individuals involved in a hoax on the campus of the University of Missouri that seemed to match the methods of the Russian trolls interviewed by Chen. I mention only one particular user in this paper, but I also monitored a dozen or so accounts that contributed to that hoax. Each account followed a pattern that also happened to align with noted Russian influence operations in Europe and eventually in the US presidential election. I describe that transition below. From those accounts, I built a database of suspected Russian bot accounts to build the network map in Figure 13. The Mizzou hoax was a trend hijacking effort launched by actors who later proved to match the Russian modus operandi of using cyber trolls originally observed by Adrian Chen, and confirmed by the ODNI report and Foreign Policy Research Institute Fellow Clint Watts in his testimony before the Senate Intelligence Committee.

outside of that attack. The narrative was set as the trend was highjacked, and the hoax was underway.

The rapidly spreading image of a bruised little boy was generating legitimate outrage across the country and around the world. However, a quick Google image search for "bruised black child" revealed the picture that "Jermaine" attached to the tweet was a picture of an African-American child who was beaten by police in Ohio over one year earlier. The image and the narrative were part of a larger plot to spread fear and distrust. It worked.

The University of Missouri student body president tweeted a warning to stay off the streets and lock doors because "KKK members were confirmed on campus." National news networks broke their coverage to get a local feed from camera crews roaming Columbia and the campus looking for signs of violence. As journalists continued to search for signs of Klan members, anchors read tweets describing shootings, stabbings, and cross-burnings. In the end, the stories were all false.

Shortly after the disinformation campaign at Mizzou, @Fanfan1911 changed his display name from Jermaine to just "FanFan" and the profile picture of a young black male changed to the image of a German iron

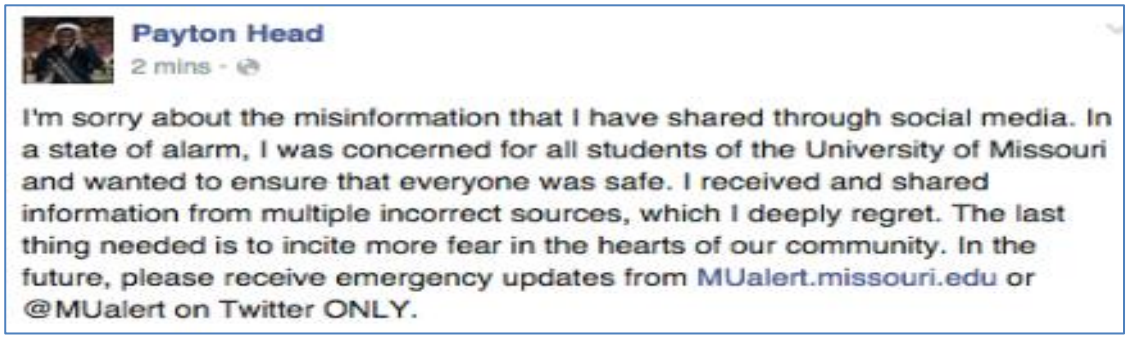


Figure 10. Mizzou student body president's apology on Facebook
Source: Facebook screenshot

cross. The next few months FanFan's tweets were all in German and consisted of spreading rumors about Syrian refugees. Russian active

measures in Europe around this time were widely reported, and the account that previously tweeted disinformation regarding Mizzou now focused on anti-Islamic, anti-EU, and anti-German Chancellor Angela Merkel messages. His tweets reached a crescendo after reports of women being raped on New Year's Eve 2016. Some of the reports were false, including a high-profile case of a 13-year-old ethnic-Russian girl living in Berlin who falsely claimed that she was abducted and raped by refugees.[15] Once again, Russian propaganda dominated the narrative.[16]

Like in previous disinformation campaigns on Twitter, the Russians trolls were able to spread the information because of an underlying fear and an existing narrative that they were able to exploit. The trolls used trend highjacking techniques in concurrence with reporting by Russian state-funded television Russia Today (RT) network. To attempt to generate more attention to the Russian anti-Merkel narrative in European media, Russian Foreign Minister Sergey Lavrov accused German authorities of a "politically correct cover-up" in the case of the Russian teen.[17]

Because of the Russian propaganda push, the anti-immigration narrative began spreading across traditional European media.[18] In fact, a magazine in Poland devoted an entire issue to the topic of Muslim immigration with a disturbing cover photo entitled "Islamic Rape of Europe" (Figure 11).

---

[15] Nadine Schmidt and Tim Hume, "Berlin teen admits fabricating migrant gang-rape story, official says." CNN.com, February 1, 2016.
[16] Judy Dempsey, "Russia's Manipulation of Germany's Refugee Problems." Carnegie Europe, January 28, 2016.
[17] Schmidt and Hume, "Berlin teen admits fabricating migrant gang-rape story, official says."
[18] Barbara Tasch, 'The aim is to weaken the West': The inside story of how Russian propagandists are waging war on Europe. *Business Insider*. February 2, 2017.

Figure 11. "Islamic Rape of Europe"
Source: *wSieci* Magazine

In addition to the German tweets, FanFan began tweeting in English again in the spring of 2016. His tweets and the tweets of other Russian trolls were spreading in America. The narrative spread by the trolls was developing a symbiotic relationship with American right-wing news organizations like Breitbart and its followers on social media—a group of true believers in the Russian propaganda narrative.

Additionally, the troll network already seeded various social media platforms with pages designed for spreading disinformation.[19] Seemingly patriotic American Facebook pages linked articles to RT, legitimate American news sources advocating a right-leaning perspective, Breitbart, right-wing conspiracy sites like InfoWars, and non-factual news sites like The Conservative Tribune and Gateway Pundit. The Facebook pages also linked to Russia-run sites with nothing but false news stories. Based on Anti-Obama sentiment, the Facebook pages were popular amongst conservative users, but not getting broad exposure. As the 2016 campaign began in earnest, much of the online animosity was now directed at Obama's potential successor: Hillary Clinton, who, in the summer of 2016 gave a speech that became a

[19] Chen, "The Agency."

rallying cry for Trump supporters, and a force-multiplying tool for the Russian trolls.

The Deplorable Network

In a September speech, Hillary Clinton made the following remark to a group of potential donors:

> You know, to just be grossly generalistic, you could put half of Trump's supporters into what I call the basket of deplorable. Right? The racist, sexist, homophobic, xenophobic, Islamaphobic—you name it. And unfortunately there are people like that. And he has lifted them up. He has given voice to their websites that used to only have 11,000 people—now 11 million. He tweets and retweets their offensive hateful mean-spirited rhetoric. Now, some of those folks—they are irredeemable, but thankfully they are not America.

Clinton went on in the same speech to say that the other half of Trump's supporters were just people who felt the system had left them behind, who needed support and empathy. Clearly, she was not referring to all of Trump's supporters as deplorable, but the narrative quickly changed after social media users began referring to themselves as "Deplorable" in their screen names.

Before the "basket of deplorables" comment, the trolls primarily used an algorithm to respond to a tweet from Donald Trump rapidly. Those tweets were prominently displayed directly under Trump's tweet if a user clicked on the original. Those users became powerful voices with large followings; Trump himself frequently retweeted many of those users.[20] However, after the Clinton speech, a "people search" on Twitter for "Deplorable" was all one needed to suddenly gain a network of

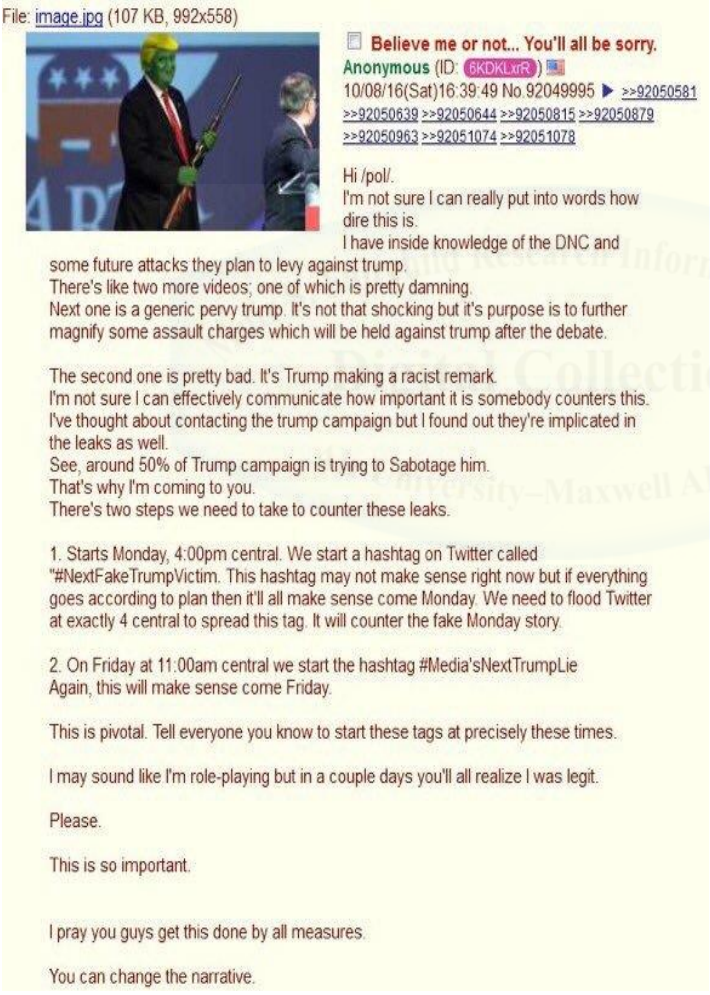
[20] K. Thor Jensen, "Inside Donald Trump's Twitter-Bot Fan Club" *New York Magazine.* June 15, 2016.

followers numbering between 3,000 and 70,000. Once again, FanFan's name changed, this time to "Deplorable Lucy" and the profile picture became a white middle-aged female with a Trump logo at the bottom of the picture. The FanFan follower count went from just over 1,000 to 11,000 within a few days. His original network from the Mizzou and European campaigns changed as well: tracing his follower trail again led to the same groups of people in the same network, and they were all now defined by the "Deplorable" brand. In short, they were now completely in unison with a vast network of other Russian trolls, actual American citizens, and bot accounts from both countries on Twitter.

With a large network consisting of Russian trolls, true believers, and bots, it suddenly became easier to get topics trending with a barrage of tweets. The Russian trolls could employ the previously used tactics of bot tweets and hashtag highjacking, but now they had the capability to create trends.

Besides creating trends, the trolls could relay strategy under the radar using Twitter. That is to say, a message could be delivered in the form of a picture that did not include any words. The lack of words would spread the message to the followers in a timeline, but retweets would not develop any trends—only that network of followers or someone actively observing the network saw the messages. Often, anonymous users discussed the tactics behind the trend creation on the social media site 4Chan, on the bulletin board called "/pol/" and subsequently coordinated the trend within the Deplorable Network on Twitter. The most effective trends derived from this strategy came in the days following the "Access Hollywood" tape release in which Donald Trump implied that he was able to touch women inappropriately because of his fame. The Deplorable Network distributed the corresponding strategy throughout the network (Figure 10) to drown out negative attention to Trump on Twitter.

Coinciding with the implementation of the strategy to mask anti-Trump comments on Twitter, WikiLeaks began releasing John Podesta's stolen emails. The emails themselves revealed nothing truly controversial, but the narrative that the trending hashtag created was powerful. First, the issue of hacked emails developed into a narrative conflating Podesta's emails to the issue of Clinton's private email server. The Clinton server was likely never hacked, but the problem of email loomed over the candidate as an indicator of her seemingly omnipresent issues of corruption. The corruption narrative also plagued the Democratic National Committee (DNC), which experienced a hack earlier in the year, also by Russian sources and revealed by WikiLeaks.[21]


File: image.jpg (107 KB, 992x558)

Believe me or not... You'll all be sorry.
Anonymous (ID: 6KDKLxrR)
10/08/16(Sat)16:39:49 No.92049995 ▶ >>92050581 >>92050639 >>92050644 >>92050815 >>92050879 >>92050963 >>92051074 >>92051078

Hi /pol/.
I'm not sure I can really put into words how dire this is.
I have inside knowledge of the DNC and some future attacks they plan to levy against trump.
There's like two more videos; one of which is pretty damning.
Next one is a generic pervy trump. It's not that shocking but it's purpose is to further magnify some assault charges which will be held against trump after the debate.

The second one is pretty bad. It's Trump making a racist remark.
I'm not sure I can effectively communicate how important it is somebody counters this.
I've thought about contacting the trump campaign but I found out they're implicated in the leaks as well.
See, around 50% of Trump campaign is trying to Sabotage him.
That's why I'm coming to you.
There's two steps we need to take to counter these leaks.

1. Starts Monday, 4:00pm central. We start a hashtag on Twitter called "#NextFakeTrumpVictim. This hashtag may not make sense right now but if everything goes according to plan then it'll all make sense come Monday. We need to flood Twitter at exactly 4 central to spread this tag. It will counter the fake Monday story.

2. On Friday at 11:00am central we start the hashtag #Media'sNextTrumpLie
Again, this will make sense come Friday.

This is pivotal. Tell everyone you know to start these tags at precisely these times.

I may sound like I'm role-playing but in a couple days you'll all realize I was legit.

Please.

This is so important.

I pray you guys get this done by all measures.

You can change the narrative.

Figure 12. Coordinating hashtag creation
Source: Screenshot of 4Chan post circulated on Twitter

Secondly, the Podesta email narrative took routine issues and made them seem scandalous. The most common theme: bring discredit to the mainstream media. John Podesta, like any campaign manager in modern politics, communicated with members of the press. Emails communicating with reporters were distributed via trending tweets with

[21] ODNI Report, 2.

links to fake news websites. The fake news distorted the stolen emails into conspiracies of media "rigging" of the election to support Hillary Clinton.

Finally, the stolen emails went beyond sharing on social media. The trend became so sensational that traditional media outlets had to cover the Podesta email story, which gave credibility to the fake news and the associated online conspiracy theories promulgated by the Deplorable Network. The WikiLeaks release of the Podesta emails was the peak of Russian command of the trend during the 2016 election. Nearly every day #PodestaEmail trended as a new batch of supposedly scandalous hacked emails made their way into the mainstream press.

By analyzing the followers of a suspected Russian troll, a picture emerges regarding the structure of the network that was active during the 2016 election. The core group in the Deplorable network consisted of Russian trolls and popular American right-wing accounts like Jack Posobiec, Mike Cernovich, and InfoWars editor Paul Joseph Watson. Figure 13 is a network map of the Deplorable Network, which combines the followers of two bot accounts to graph the overlapping followers of the two accounts. The small cluster in the center is the core group; the ring that surrounds it is the bot network.

The remaining nodes are individual accounts likely consisting of human-managed accounts; the accounts in the middle have more followers, the outside accounts with weaker links have fewer followers. In total, the Deplorable Network was approximately 200,000 Twitter accounts consisting of Russian trolls, true believers, and bots. Based on my analysis, the bot network appeared to be between 16,000-34,000 accounts. [22]

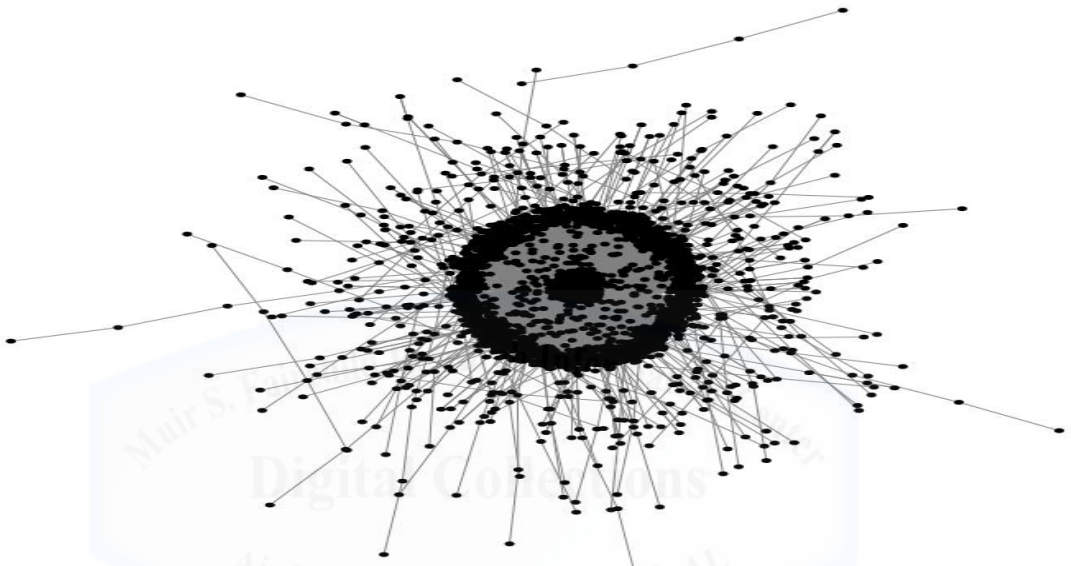


Figure 13. Network of two accounts
Source: Author

Figure 14 shows what the Deplorable Network looks like within the larger spectrum of American political networks on Twitter. The bright red clusters in the lower right of the network map were accounts that only followed Donald Trump. The cohesiveness of the group indicates how a coordinated effort can create a trend in a way that a less cohesive

[22] This count is based on analysis of the followers of followers of suspected troll accounts and bots. The study was conducted on March 15, 2016. The number of accounts appears to have reduced dramatically since May, following the French election, implying that Twitter suspended some of the accounts. Unfortunately, software limitations prevent this analysis from being more accurate. Additionally, it is nearly impossible to derive the exact number of Russian accounts from that network using my available resources.

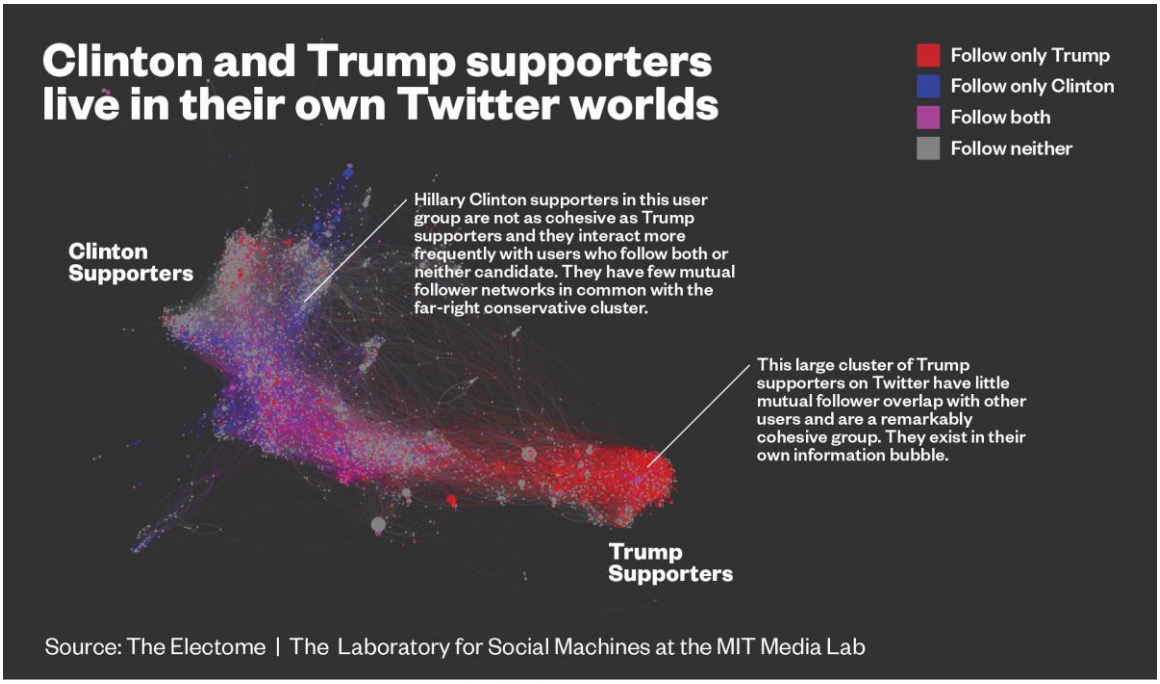


Figure 14. Network map of Clinton and Trump supporters
Source: "Parallel Narratives" Alex Thompson, Vice News

network could not accomplish. To conduct cyber-attacks using social media as a weapon, an organization must have a vast network of bot accounts in order to take command of the trend.

Summary

One month after the election, a man drove from his home in North Carolina to Washington, DC to uncover the truth behind a news story he read online. He arrived at Comet Ping-Pong pizza with an AR-15, prepared to free children from an underground child sex trafficking ring in the restaurant. After searching the store, he found no children. The story was a hoax.

One of the emails stolen from John Podesta was an invitation to a party at the home of a friend that promised good pizza from Comet Ping Pong and a pool to entertain the kids. Fake news sites reported the email as code for a pedophilic sex party; it was widely distributed via the

trending #PodestaEmail hashtag and an associated new hashtag, #PizzaGate.

The #PizzaGate hoax, along with all of the other false and quasi-false narratives became common within right-wing media as another indication of the immorality of Clinton and her staff. Often, the mainstream media would latch onto a story with unsavory backgrounds and false pretenses also, thus giving more credibility to all of the fake news; however, the narrative from the #PizzaGate hoax followed the common propaganda narrative that the media was trying to cover up the truth, and the government failed to investigate the crimes. Ultimately, that is what drove the man to inquire into the fake news for himself.[23]

With unknown factors like the impact of fake news, the true results of the Russian influence operation will likely never be known. As Ellul said, experiments undertaken to gauge the effectiveness of propaganda will never work because the tests "cannot reproduce the real propaganda situation."[24] The concept itself is marred by the fact that much of the social media support Trump received was through real American true believers tweeting. However, two numbers will stand out from the 2016 election: 2.8 million and 80,000. Hillary Clinton won the popular vote by 2.8 million votes, and Donald Trump won the electorate via a combination of just over 80,000 votes in three key states. One could easily make the case—as many on the left have done—that Hillary lost because of the Russian influence.[25] Conversely, one could also argue that Clinton was a flawed candidate and she was destined to lose because of a

---

[23] Faiz Siddiqui and Susan Svrluga, "N.C. man told police he went to D.C. pizzeria with gun to investigate conspiracy theory." *Washington Post*, December 5, 2017.
[24] Ellul, 6.
[25] Many on the left have mischaracterized the attack as "Russian hacking of the election," which has in turn conflated the issue of the John Podesta email theft with a hacking of the actual election systems. To be clear: there is no evidence of any sort of hack on any ballot counting systems, only evidence outlined in this paper of two hacks (DNC and Podesta) combined with an influence/information operation.

botched campaign combined with a growing sense of disenchantment with the American political system. However, one cannot dispute the fact that Russia launched a massive cyber warfare campaign to influence the election for Donald Trump.[26]

Hillary Clinton has been a target of political scorn from conservative groups since she first came into the national spotlight as First Lady in the 90s. Claiming she and her husband were victims of a "vast right-wing conspiracy" early in President Clinton's first term seemed hyperbole at the time.[27] Throughout his presidency, however, the Clinton name became synonymous with scandal, and that reputation would follow Hillary into her political foray. Ultimately, groups on the left and right presented strong opposition to her candidacy in 2016, which meant that Russian trolls already had a narrative to build upon and a network of true believers on social media to spread their propaganda.

Obviously, that network ultimately became the Deplorable Network, which also included scorned Bernie Sanders supporters, the "Bernie Bros." Together, the Russian cyber trolls combined efforts with American Twitter accounts to discredit Hillary Clinton. Additionally, the Russian trolls spread Russian propaganda to bolster Putin's image—particularly regarding Russian involvement in Syria.[28]

For the most part, the Russian trolls became savvier with their techniques as they adapted to the influence operation in the United States. However, some users, like FanFan, were sloppy with their tradecraft and were obvious to anyone monitoring. The trolls were occasionally sloppy with their IP address locations as well. Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly

---

[26] ODNI Report, 1
[27] Hanna Rosin, "Among the Hillary Haters." *The Atlantic.* March 1, 2015, 63.
[28] Meyer "War Goes Viral."

noticed that the worldwide hashtag seemed to originate in St. Petersburg, Russia.

Russian trolls gave obvious support to Donald Trump, but the operation also included other benefits for Russia despite the winner of the Presidency: Russia proved that using social media as a weapon could create chaos on a massive scale, discredit any politician, and divide American society. An additional benefit for Russia is the more favorable view of Russian policy and Vladimir Putin and Russia as a whole. Recent surveys indicate that an uptick in American opinions of Russia in 2016 (Figure 11), especially amongst Republican voters, of whom only 12% saw Putin favorably in 2015, versus 32% in 2017.[29]

Adrian Chen, the New York Times reporter who originally uncovered the troll network in St. Petersburg in 2015, went back to Russia in the summer of 2016. Russian activists he interviewed claimed that the purpose of the trolls "was not to brainwash readers, but to

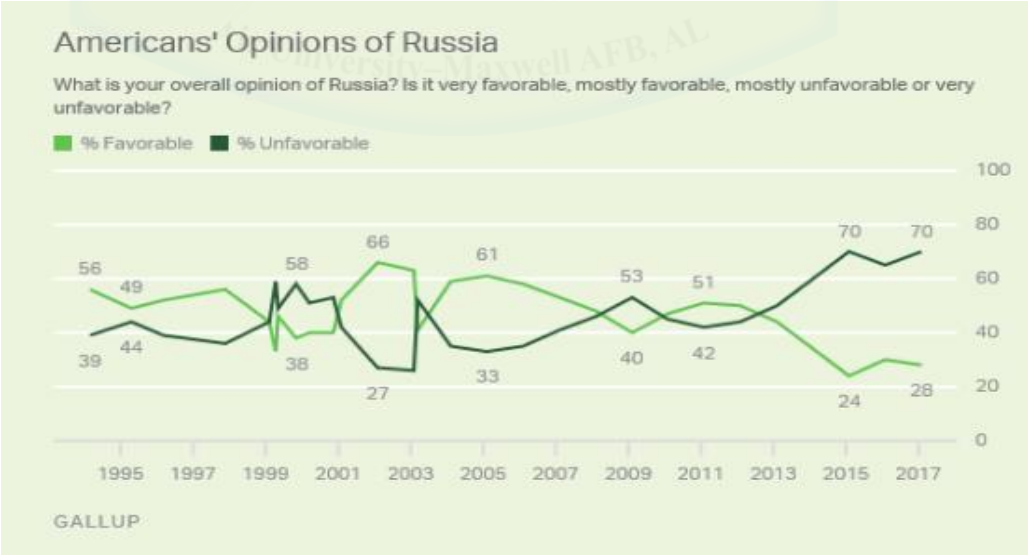


Figure 15. Americans' Opinions of Russia
Source: Russia Historical Trends, Gallup

[29] Chris Cillizza, "Analysis: Vladimir Putin's popularity is soaring among Republicans." *The Washington Post.* February 21, 2017.

overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[30] The troll farm used similar techniques to drown out anti-Putin trends on Russian social media in addition to pumping out disinformation to the United States.

A Congressional Research Service Study summarized the Russian troll operation succinctly in a January 2017 report: "Cyber tools were also used [by Russia] to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the democratic process itself."[31]

To Russia, information warfare is a specialized type of war, and modern tools make social media the weapon. According to a former Obama administration senior official, Russians regard the information sphere as a domain of warfare on a sliding scale of conflict that always exists between the US and Russia.[32] This perspective was on display during a Russian national security conference "Infoforum 2016." Andrey Krutskih, a senior Kremlin advisor, compared Russia's information warfare to a nuclear bomb, which would allow Russia to talk to Americans as equals," in the same way that Soviet testing of the atomic bomb did in 1949.[33]

Table 4. Russia Case Study Analysis in 2016 Election

Propaganda Narratives	1. Anything discrediting to Hillary Clinton 2. News media hides information

[30] Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks." *The New Yorker*. July 27, 2016.
[31] Catherine Theohary and Cory Welt. 2017. Russia and the U.S. Presidential Election. CRS Report No. IN10635. Washington, DC: Congressional Research Service.
[32] David Ignatius, "Russia's radical new strategy for information warfare." *Washington Post*. January 18, 2017
[33] Ignatius.

	3. Politicians are rigging the system 4. Global elite trying to destroy the world 5. Globalism is taking jobs and destroying cultures 6. Refugees are terrorists 7. Russian foreign policy is strong on anti-terrorism 8. Democrats and some Republicans want WWIII with Russia
True Believers	Alt-right, some Bernie Sanders supporters, followers of Info Wars and Breitbart, 4Chan /pol/ users.
Cyber Warriors	Hackers and professional trolls
Bot Network	Large, sophisticated network that leveraged cyber warriors and true believer accounts to create the "Deplorable Network."

Source: Author

From 2015-2016, Russian trolling modus operandi took a logical path from small stories designed to create panic and sow seeds of doubt, to a social media machine that ISIS could only imagine. In warfare strategy, narrative manipulation through social media cyber operations is the current embodiment of Douhet's theory of taking the fight directly to the people. The 2016 election proved that using social media to influence political outcomes, as opposed to violence or Cold War-like posturing, is a highly effective strategy in modern warfare—a strategy that will likely continue as technology continues to develop and adapt to the ever-growing social media landscape as more actors gain the ability to take command of the trend.

Chapter 4

The War of 20—

Right now in Moscow, they must be clinking vodka glasses. Because for less than the cost of a MiG-29, they have thrown the West into complete disarray.

Thomas Freidman on *Meet the Press*, 2017

The young congresswoman rolled out of bed later than anticipated on her first Monday back in Washington after a busy weekend. Her schedule had been packed since the previous Thursday when she co-sponsored a bill to increase funds for federal employee cyber awareness training right after taking to the floor as the leading advocate for military action in a troubled part of the world. The next day was an awards ceremony, followed by dinner at the State Department honoring the 2019 International Women of Courage (IWC), who were recognized for their courageous stands in the face of adversity from their governments. All that before catching a late flight back to her district to spend the rest of the weekend with her chief of staff filling out paperwork and registering online domain names for her 2020 Senate run.

She was polling off the charts in her state, and she was looking forward to another productive week to show off her skills in Washington to her constituents back home. Over coffee, she unlocked her phone to see a red circle with "27.5K" over her Twitter application. Odd, she thought, normal Twitter traffic to her account usually numbered only a few dozen. Suddenly, a chill ran through her spine. As a member of the House Intelligence Committee, and a self-proclaimed cyber expert, she had seen things like this before, and now she was certain that she was a victim of an online smear campaign. Without reading any of the

messages that included her Twitter handle, she looked at the trends. The top five trends at that moment: her name, #terroristincongress, "congresswoman speech," "WWIII," and "proof of abortion."

The narrative produced by those trends was an odd combination of complete falsehoods mixed with small amounts of truth. First, one trend revealed hacked emails that she told her chief of staff that she "didn't want to go back to that place because of what happened there in college." In reality, she was talking about not wanting to campaign at an in-state rival university that beat her and her volleyball team when she was in college, but the narrative was that she had an abortion. The trend "proof of abortion" included forged documents and grotesque pictures as evidence of her alleged college experience. Additionally, some of her old tweets from college were being retweeted, each of which she thought she deleted when she first ran for office because the content made it seem like she partied too much over one particular spring break.

Secondly, "congresswoman speech" linked to a Washington Post article that mentioned her floor speech the previous week. The trend was a combination of average people sharing the link, and nefarious bot accounts that included the words "congresswoman speech" with a narrative that she was trying to start WWIII. Of course, those tweets were the genesis of the other trend, "WWIII."

Most frighteningly of all of the trends was that the WWIII trend also claimed she was trying to unite with terrorists to fight WWIII. The tweets included a video of her wearing a headscarf in a tent with Middle Eastern Jihadists. The end of the video shows the group praying together, and includes the audio of her voice saying, "I pray with you, and support you always." These tweets included the last trend, #terroristincongress.

She had never met with any Jihadists on any of her trips to the Middle East, and she had certainly never uttered those words; yet, it appeared to be her in the first scene of the video, and her voice was loud

and clear in the second. She remembered that she had a still-photo with a Muslim woman at the IWC event the previous week. The woman gave her a headscarf as a gift, and she wore it briefly for the photo.

She turned on her television. Every morning show was talking about her. Because the story broke on Monday, she already knew that the 24-hour cable news networks would cover her alleged scandals for the rest of the week. The congresswoman's reputation was shattered. She could easily deny all of the claims, but this barrage attack on her character and her motives would most likely kill her future political ambitions—and the policy agenda she outlined in Congress.[1]

Old Meets New

Douhet titled the final chapter of his book "The War of 19—." The conclusion was a fictional account of how he believed the next war would be fought based on his assessment of current technology. His story included the notion that future wars would end once a side gained command of the air, subsequently influencing the will of the population to demand their government change the state's strategic direction. The fictional account to start this chapter is a very real possibility based on current technology and the use of social media as a weapon by gaining command of the trend to influence the will of the population to change the state's strategic direction. In the example, a rising star in politics was smeared. Her agenda included a strong foreign policy against an

[1] Each trend in the fictional account is based on similar attacks on Twitter of various public figures. One thing worth noting is the fake video. Current technologies used by some social media apps, like Snapchat, create an "augmented reality." As this technology advances, scenes like this fictional account will be able to be created by anyone with a smart phone and a picture of the target. Additionally, various "lip-dub" and "auto-tuned" parody videos are generally entertaining, but a bad actor could easily use those same techniques to create audio forgeries. Washington Post technology columnist Avi Selk recently previewed of this new technology in his article "This audio clip of a robot as Trump may prelude a future of fake human voices."

adversary, and she was a leading voice of military action against that particular country. Those plans would be sidelined after a targeted campaign distracting the country with falsehoods.

Smear campaigns have been around since the beginning of politics, but the fictional example in this paper illustrated novel techniques recently employed by foreign state actors and terrorist groups, with each attack gaining popularity and credibility after trending on Twitter. The attacks, often under the guise of a "whistleblower" campaign, make the routine seem scandalous. Additionally, WikiLeaks advertises that they have never published anything requiring retraction because everything they have posted is supposedly authentic stolen material. Just like the Podesta email releases, several politicians and business leaders around the world have fallen victim to this type of attack.

People likely remember the 2015 North Korean hacking of Sony Studios to retaliate for a movie depicting the assassination of Kim Jong-un. Lost in the explosive nature of the hacking story is that the fallout at the company was not because of the hacking itself but from the release of embarrassing emails from Sony senior management, as well as the salaries of every employee at Sony. The uproar over the content of the emails dominated social media, often fed by salacious stories like the RT headline: "Leaked Sony emails exhibit wealthy elite's maneuvering to get child into Ivy League school." Ultimately, Sony fired a senior executive because of the content of her emails.[2]

As I write this theory of future warfare, the French are going to the polls to elect a new president only 48-hours after nine gigabytes of email stolen from the Emmanuel Macron campaign were released online and verified by WikiLeaks. Subsequently, the hashtag #MacronLeaks rose to the number one worldwide trend in an influence operation resembling

[2] "Ex-Sony Chief Amy Pascal Acknowledges She Was Fired." NBCNews.com, February 12, 2015

the #PodestaEmail campaign with a supporting cast of some of the same actors.

I have observed during the weeks preceding the French Election that many accounts within the Deplorable Network have changed their names to support Macron's opponent, Marine LePen. These accounts mostly Tweet in English and still engage in American political topics as well as French issues. Some of the accounts also Tweet in French and a new network of French-tweeting bot accounts uses the same methods as the Deplorable Network to take command of the trend. Additionally, the political left in the United States seems to have a large group of bot accounts forming around the "Resist" movement. To this point, it is unclear whether those accounts are foreign cyber warriors or bots, but external actors can certainly feed off the underlying narratives and tap into existing networks of true believers.

Actors like North Korea and Russia have significantly more resources and are better equipped to exploit social media than their non-state counterpsrts; still, as Chapter 2 demonstrated, non-state actors like ISIS can use social media as a weapon to spread propaganda, which bolsters recruiting in addition to serving as a low-cost pseudo-terror attack without actually committing any resources toward international terrorism.

Future Warfare

In his book, *Out of the Mountains*, David Kilcullen describes a future comprised of large, coastal urban areas filled with potential threats, all connected.[3] The implications of his prediction are two-fold. First, networks of malicious non-state actors can band together to

[3] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*. (New York: Oxford University Press, 2013), 231.

weaponize social media using a template similar to ISIS. Although these groups may not have the power to create global trends, they can certainly create chaos with smaller numbers by hijacking trends and creating local trends. With minimal resources, a small group can create a bot network to amplify its message. Second, scores of people with exposure to social media are vulnerable to online propaganda efforts. In this regard, state actors can use the Russian playbook.

Russia will likely continue to dominate this new battlespace. Russia has intelligence assets, hackers, cyber warrior trolls, massive bot networks, state-owned news networks with global reach, and established networks within the countries Russia seeks to attack via social media. Most importantly, the Russians have a history of spreading propaganda using a method they perfected—active measures and disinformation.

After the 2016 elections in the United States, Russian trolls again worked toward influencing European elections. Currently, Russian trolls are active in France, the Balkans, and the Czech Republic using active measures and weaponized social media messages.[4] It is clear that other countries are attempting to build capabilities to match the Russian cyber troll influence.

Already, Turkey, Iran, and Venezuela are noted as having bot networks and cyber warriors similar to Russian trolls.[5] With these other states, a popular use for the trolls in the social media battlespace is to stoke nationalism and control the narrative within their own borders. For example, the fake Twitter followers of Venezuelan President Nicolás Maduro number so many that he is now the "third-most-retweeted public figure in the world, behind only the king of Saudi Arabia and the pope."[6]

---

[4] Anthony Faiola, "As Cold War turns to Information War, a new fake news police combats disinformation." *The Washington Post,* January 22, 2017.
[5] Meyer, "War Goes Viral."
[6] Meyer, "War Goes Viral."

With a large enough bot network, states can also control messages outside of social media using similar techniques. Manipulating search engines is called “search engine optimization,” which uses bot accounts to increase the number of clicks to a particular web page after performing a search. The search engine algorithm then prioritizes that page in response to subsequent searches using the same keyword.

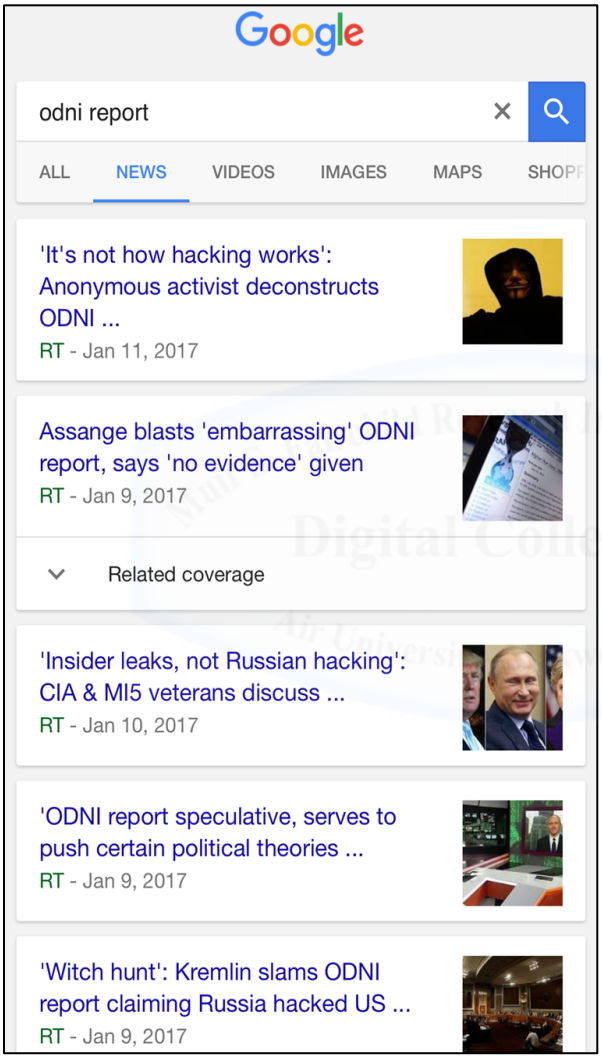


Figure 16. Google Search of "ODNI Report"
Source: Author screenshot

Figure 15 shows a screen capture of a Google search for “ODNI Report.” All of the results are RT articles lambasting the intelligence assessment that named the Russian government as the perpetrators behind the 2016 election interference.

Techniques like search engine optimization and command of the trend will become common in future wars to sow discord and spread false information, with the aim of causing the other side to change its course of action. These online weapons should frighten every leader in a democracy. Perhaps most frightening is the Oxford Internet Institute Unit for Propaganda discovery that “hundreds of thousands of ‘sleeper bots’ exist on Twitter.” [7] These bots are accounts that are active

[7] Cadwalladr, 18

but have not yet started tweeting. Researchers do not know who owns the accounts, or what will trigger them.

The ease of use and large numbers of active bots and sleeper bots indicate a high likelihood of social media continuing to be used as a weapon, especially as more and more state and non-state organizations realize the impact they can make on an adversary. ISIS and Russia are models for this future war that uses social media as a weapon. As technology improves, techniques are refined, and internet connectivity continues to proliferate around the world, this saying will once again ring true: he who controls the trend will control the narrative, and ultimately the narrative controls the will of the people.

Conclusion

In the 1987 book, *Truth Twisters*, Richard Deacon laments the future of independent thinking, as computers "could become the most dangerous hypnotic influence in the future. Allowing oneself to be manipulated and controlled by it."[1] He believed that such technology could lead one to commit treason without realizing any manipulation. Propaganda is a powerful tool and, used effectively, it has been proven to manipulate populations on a massive scale. The weaponization of social media and the command of the trend make the spread of propaganda easier than ever before for both state and non-state actors.

Certainly, the spread of propaganda is faster, cheaper, and has a wider reach due to the confluence of technical and social factors. Web 2.0 allowed the average internet user to go from consumer of information to producer of information. From that, the rise of social media as a network builder solidified viewpoints existing within each homophilic network. Then, blogs, video uploads, and social media enabled the "citizen reporter." Suddenly, anyone with an opinion and internet access could share his or her thoughts with anyone within their network willing to listen.

Occurring simultaneously with social media's rise in popularity was the shift from print media to online media. Social media allowed users to scan and share stories to their followers quickly. For journalists, the movement of news to social media forced them to adapt their content to a more "clickable" style—shorter headlines, frequent posting, and more hyperbole to compete with other journalists as well as popular bloggers. Journalists also began using social media—particularly Twitter—as a source for breaking news. The result was questionable

[1] Richard Deacon, *The Truth Twisters*. (London: Macdonald, 1987), 95.

content could make its way to journalists who were quick to push narratives without verification, in an attempt to compete with other voices on Twitter. In short, social media can now weaponize fake news, which could find its way into the real news.

The problem with using social media as a weapon is the structural hole. Generally, networks of opinions tend to isolate themselves, creating an echo chamber of thoughts and ideas. Homophily has been both a blessing and a curse to propagandists for centuries. Propaganda is believable to an individual with a predisposition toward a particular narrative. Conversely, a person with an outside viewpoint will shun new ideas and opinions from a different perspective. In other words, the two groups were not communicating with each other online, which is evident in the map of Clinton and Trump supporters in Figure 14. To cross networks, a message must first traverse the gap between the two networks—the structural hole—social media enables that form of information sharing with the trending topics list. For anyone trying to spread propaganda, the trending tool became the most efficient method.

ISIS was the first organization to harness the power behind the trend. Without a doubt, ISIS' presence online gave the group an air of strength and power that the group did not have. The ISIS brand, combined with a cleverly designed bot network capable of hijacking and creating trends, made the group seem as if it were an existential threat worldwide. The group itself does not claim to be a terrorist organization, but terror threats through trends spread their propaganda containing horrifying images of their brutal executions, which, in turn, served as de facto acts of terror. Additionally, the group thrived off the recruiting potential of social media using the same messaging and branding techniques. ISIS proved that a non-state organization could weaponize social media by taking command of the trend to meet their objectives.

Regarding state actors, Russia is, and always has been, the biggest player in the worldwide spread of propaganda. Dating back to the Cold

War, the Soviets developed a style of spreading false information that uses a variety of resources to disseminate disinformation. Russian active measures are still in use today and are made more powerful through the use of social media. Russia's military organization of cyber trolls, hackers, and botnets highlights the state focus of resources and efforts in the information domain.

While Russia is the largest state actor with the ability to take command of the trend, others are joining. Several countries are using the Russian template to build their disinformation cyber trolls, and the existence of new bot accounts demonstrates that future warfare will continue to include social media as a weapon in the information warfare domain.

Thus far, the United States response has been relatively weak. For one thing, the United States government does not prioritize information operations the way it once did during the Cold War. When Eisenhower started the United States Information Agency, the objective was to compete with Soviet propaganda around the world. The mission statement of USIA clarified its role: "The purpose of the United States Information Agency shall be to submit evidence to peoples of other nations by means of communication techniques that the objectives and policies of the United States are in harmony with and will advance their legitimate aspirations for freedom, progress, and peace."[2]

Knowing what we know now about Russian disinformation active measures, USIA was never truly equipped to fight an information war. The agency became a public diplomacy platform with a positive message, not the negative smear tactics the Soviets were using to attempt to discredit the United States. Accordingly, several questions arose at that time: should USIA spread propaganda? Should it seek out and attempt to

---

[2] Malcolm Mitchell, *Propaganda, Polls, and Public Opinion: Are the People Manipulated?* (Englewood Cliffs, N.J.: Prentice-Hall, 1977), 12.

remove negative publicity about the US? Should it slander opponents? Most importantly: should it do any or all of these things when the American public could be influenced by a message intended for an international audience?[3]

Those problems still exist today, and the government lacks a centralized information authority since the mission of USIA was relegated to the Department of State. Several failed attempts to counter ISIS on Twitter show the weakness that the US government has when trying to use social media as a weapon. One example is through the Center for Strategic Counterterrorism Communications, created in 2010, which started the program "Think Again Turn Away," and awarded a $575,046 contract to a Virginia-based consulting firm to manage the project.[4] The intent was to curb the appeal of ISIS by creating a counter-narrative to the ISIS message on social media. Unfortunately, the Twitter campaign had undesirable consequences after the account sent tweets arguing the finer points of the Islamic faith with ISIS sympathizers. Rita Katz best summarized the failure: "In order to counter a problem, one must first study it before adopting a solution. Had the people behind "Think Again, Turn Away" understood jihadists' mindsets and reasons for their behavior, they would have known that their project of counter-messaging would not only be a waste of taxpayer money but ultimately be counterproductive."[5]

In the end, the "Think Again, Turn Away" campaign was almost comical as it could not communicate effectively with any audience and severely discounted the importance of its message. Jacques Ellul noted that democracies were prone to having problems with outward

---

[3] Mitchell, 13.
[4] Rebecca Carroll, "The State Department Is Fighting With ISIL on Twitter." Defense One. June 25, 2014.
[5] Rita Katz, "The State Department's Twitter War with ISIS Is Embarrassing." *Time Magazine*, September 16, 2014.

communication through propaganda. Because democracies rely on presenting an image of fairness and truth, "propaganda made by democracies is ineffective, paralyzed, mediocre."[6] The United States was ill-equipped to combat Soviet active measures during the Cold War, and we remain unable to compete using social media as a weapon.

Unfortunately, countering Russian influence operations has taken a partisan slant as well. Many Republicans downplay the Russian role in the 2016 election because admitting the effects could weaken the political capital of President Trump's administration. On the other hand, Democrats appear to be so blinded by the Russian operation that they cannot see the underlying conditions that allowed for the spread of that narrative in the first place.[7] With the two parties unable to reach a consensus on what happened and the impact of the operation, they fail to realize that as technology improves and proliferates around the world, disinformation campaigns and influence ops will become the norm. The fictional candidate at the beginning of Chapter 4 could be from either party, and the attack in a future war in the information sphere could come from any of the several countries attempting to build an online army in the mold of Russia's trolls and bot network.

Fortunately, social media companies are taking steps to combat the weaponization of their mediums. Facebook has been at the forefront of tech companies taking action to increase awareness of fake news, and a process for removing the links from the website.[8] Also, although Facebook trends are less important to information warfare than Twitter trends, the website has taken measures to ensure that humans are involved in making the trends list. Furthermore, Twitter has started discreetly removing unsavory trends within minutes of their rise in

---

[6] Ellul, 241.
[7] Adrian Chen, "The Propaganda about Russian Propaganda" *The New Yorker*, December 1, 2016.
[8] Michelle Castillo, "Facebook found fake accounts leaking stolen info to sway presidential election." CNBC.com, April 27, 2017.

popularity. Of course, adversaries adapt in warfare; thus, Twitter trolls have attempted to regain command of the trend by misspelling a previous trend once it is taken out of circulation. Still, even if the misspelled word regains a spot on the trend list, the message is diminished.

The measures enacted by Facebook and Twitter are important for preventing future wars in the information domain. However, Twitter will also continue to have problems with trend hijacking and bot networks. As demonstrated by #PrayforMizzou and #WorldCup2014, real events happening around the world will maintain popularity as well-intending users want to talk about the issues. In reality, removing the trends function could end the use of social media as a weapon, but doing so could also devalue the usability of Twitter. Rooting out bot accounts would have an equal effect since that would nearly eliminate the possibility of trend creation. Unfortunately, that would have an adverse impact on advertising firms who rely on Twitter to generate revenue for their products.

With social media companies balancing the interests of their businesses and the betterment of society, other intuitions must respond to the weaponization of social media. In particular, the credibility of our press and our politicians have been put into question by social media influence campaigns—those groups should respond accordingly. For instance, news outlets should adopt social media policy for their employees which encourage the use of social media but discourage them from relying on Twitter as a source. This will require a culture shift within the press that is outside of the scope of this paper but fortunately has gathered significant attention at universities researching the media's role in the influence operation. It is worth noting that the French press did not cover the content of the Macron leaks; instead, the journalists covered the hacking and influence operation without giving any credibility to the leaked information.

Finally, our elected officials must move past the partisan divide of Russian influence in the 2016 election. This involves two things: first, both parties must recognize what happened—neither minimizing nor overplaying Russian active measures. Second, and most importantly, politicians must commit to not using active measures to their benefit. Certainly, the appeal of free negative advertising will make any politician think twice about using disinformation, but the reality of a foreign influence operation damages more than just the other party, it damages our democratic ideals. Senator John McCain summarized this sentiment well at a CNN Town Hall when he said, "Have no doubt, what the Russians tried to do to our election could have destroyed democracy. That's why we've got to pay a hell of a lot more attention to the Russians and the things they're doing in Europe—and right now, they're trying to determine the outcome of the French election, and they're using cyber."[9]

This was not the cyber war we were promised. Predictions of a catastrophic cyber-attack dominated policy discussion, but few realized that social media could be used as a weapon against the minds of the population until ISIS started spreading their propaganda in 2014. Since then, the command of the trend has gained importance in this new battlespace as Russia used social media to conduct a massive influence operation against the United States. Thus, nearly 100 years later, Douhet's idea that attacking the people would cause them to rise and demand change from their government was realized; however, the means for implementing that change was not the command of the air—it was the *Command of the Trend.*

[9] Eric Bradner, "At CNN town hall, McCain and Graham give their view of Trump's presidency so far." CNN.com, March 2, 2017.

Bibliography

Alario, Celia. “Fake Followers and Twitter Astroturf: It's Sorta Social, Demented and Sad, But Social.” *The Huffington Post*. August 9, 2011. http://www.huffingtonpost.com/celia-alario/fake-followers-and-twitter_b_919091.html.

Allcott, Hunt, and Matthew Gentzkow. *Social media and fake news in the 2016 election*. No. w23089. National Bureau of Economic Research, 2017.

Asur, Sitaram, Bernardo A. Huberman, Gabor Szabo, and Chunyan Wang. "Trends in Social Media: Persistence and Decay." Cornell University, 2011.

Attkisson, Sharyl. “Astroturf and manipulation of media messages.” TEDx video, University of Nevada, 10:36, filmed February 6, 2015.

Apuzzo, Matt. “Who Will Become a Terrorist? Research Yields Few Clues.” The New York Times. March 27, 2016.

Baker, Aryn. “How ISIS Is Recruiting Women From Around the World.” *Time Magazine.* Sept. 6, 2014. http://time.com/3276567/how-isis-is-recruiting-women-from-around-the-world/

Berger, J. M. “How ISIS Games Twitter.” *The Atlantic*. June 16, 2014. http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

——— “How ISIS Succeeds on Social Media Where #StopKony Fails.” *The Atlantic*. March 16, 2015. http://www.theatlantic.com/international/archive/2015/03/how-isis-succeeds-where-stopkony-fails/387859/

——— “ISIS and the Foreign-Fighter Phenomenon.” *The Atlantic*. March 8, 2015. http://www.theatlantic.com/international/archive/2015/03/isis-and-the-foreign-fighter-problem/387166/

——— “The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter.” Brookings Institute, March 20, 2015. http://www.brookings.edu/~/media/research/files/papers/2015/

03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

Eric Bradner, "At CNN town hall, McCain and Graham give their view of Trump's presidency so far." CNN.com, March 2, 2017. http://www.cnn.com/2017/03/01/politics/john-mccain-lindsey-graham-town-hall/

——— "ISIS using encryption to evade FBI." CNNPolitics.com. July 8, 2015. http://www.cnn.com/2015/07/08/politics/fbi-comey-isis-encryption-recruitment/index.html

Byman, Daniel. *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know*. What Everyone Needs to Know. 2015.

——— "Beyond Counterterrorism: Washington Needs a Real Middle East Policy." *Foreign Affairs* 94, no. 6 (2015): 11-18.

——— *The Five Front War: The Better Way to Fight Global Jihad*. Hoboken, NJ: John Wiley & Sons, 2008.

Cadwalladr, Carole. "Robert Mercer: the big data billionaire waging war on the mainstream media." *The Guardian*. February 26, 2017. https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage

Callimachi, Rukmini. "ISIS and the Lonely Young American." *The New York Times*. June 27, 2015. http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html

——— "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar." *The New York Times*. March 5, 2007. https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html?_r=0

Carnegie, Dale. *How to Win Friends and Influence People*. Rev. ed. New York: Simon and Schuster, 1981.

Carroll, Rebecca. "The State Department Is Fighting With ISIL on Twitter." Defense One. June 25, 2014. http://www.defenseone.com/technology/2014/06/state-department-fighting-isil-twitter/87286/

Castillo, Michelle. “Facebook found fake accounts leaking stolen info to sway presidential election.” CNBC.com, April 27, 2017. http://www.cnbc.com/2017/04/27/facebook-found-efforts-to-sway-presidential-election-elect-trump.html?utm_content=buffera9498&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Chen, Adrian. “The Agency.” *New York Times Magazine*, June 2, 2015.

——— “The Propaganda about Russian Propaganda” *The New Yorker*, December 1, 2016.

——— “The Real Paranoia-Inducing Purpose of Russian Hacks.” *The New Yorker*. July 27, 2016.

Cillizza, Chris. “Analysis: Vladimir Putin’s popularity is soaring among Republicans.” The Washington Post. February 21, 2017. https://www.washingtonpost.com/news/the-fix/wp/2017/02/21/vladimir-putin-so-hot-right-now/?utm_term=.f8cd95114a10.

Clarke, Richard A., and Knake, Robert K. *Cyber War : The next Threat to National Security and What to Do about It*. New York: Ecco, 2010.

Clausewitz, Carl von. *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976)

Close, Joshua R., and Air University. Air Command Staff College. *#Terror: Social Media and Extremism*, 2014.

Cohen, Kelly. “The Reason the U.S. Government Is Investing Huge Money in Social Media.” *Washington Examiner*. June 25, 2014.

Cole, Kaci, and Air University. School of Advanced Air Space Studies. *Turning Cyberpower into Idea Power [electronic Resource]: The Role of Social Media in US Strategic Communications*, 2011.

Cottee, Simon. “Why It’s So Hard to Stop ISIS Propaganda.” *The Atlantic*. March 2, 2015. http://www.theatlantic.com/international/archive/2015/03/why-its-so-hard-to-stop-isis-propaganda/386216/

Cronin, Audrey Kurth. *How terrorism ends: understanding the decline and demise of terrorist campaigns*. Princeton University Press, 2009.

——— "ISIS Is Not a Terrorist Group" *Foreign Policy.* March/April 2015. https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group

Cohen, Craig, et al. "2016 Global Forecast." Center for Strategic and International Studies. Nov 15, 2015. http://csis.org/publication/2016-global-forecast

Countering Violent Extremism, A Guide for Practitioners and Analysts, National Counterterrorism Center, 2014.

Cull, Nicholas. "WikiLeaks, public diplomacy 2.0 and the state of digital public diplomacy." *Place Branding and Public Diplomacy.* 2011.

"Curriculum Impact M&E Pakistan Study." Big Bad Boo Productions, 2015.

Deacon, Richard. *The Truth Twisters*. London: Macdonald, 1987.

Dearden, Lizzie. "Khalid Masood: Suspected Isis supporter used WhatsApp two minutes before London attack." *The Independent*. March 24, 2017. http://www.independent.co.uk/news/uk/home-news/khalid-masood-whatsapp-westminster-london-attack-parliament-message-isis-terror-network-contacts-a7649206.html

Dempsey, Judy. "Russia's Manipulation of Germany's Refugee Problems" Carnegie Europe, January 28, 2016. http://carnegieeurope.eu/strategiceurope/62611

Department Of State. The Office of Website Management, B. of P. A. October 1, 2014. The Global Coalition to Counter ISIL. http://www.state.gov/s/seci/index.htm

Diamond, Larry. "Liberation Technology," *Journal of Democracy* Vol. 21 No. 3. 2010.

Douhet, Giulio. *The Command of the Air* 1921; repr., Tuscaloosa: University of Alabama Press, 2009.

Echle, Christian. "#NEWACTORS, #OLDPROBLEMS" *KAS International Reports*. Sep. 7, 2015. http://www.kas.de/wf/doc/kas_42449-544-2-30.pdf?150908105638

Ellul, Jacques. *Propaganda; the Formation of Men's Attitudes.* New York: Knopf, 1965.

English, Carleton. "Twitter continues to wage its own war against ISIS." *New York Post*, March 21, 2017. http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/

Facebook. Facebook 2nd Quarter 2015 Statistics. July 29, 2015.

Faiola, Anthony. "As Cold War turns to Information War, a new fake news police combats disinformation." The Washington Post. January 22, 2017. https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html?postshare=9721485128534012&tid=ss_tw&utm_term=.1b9c9528a7e1.

Faris, David. "From the Age of Secrecy to the Age of Sharing: Social Media, Diplomacy, and Statecraft in the 21st Century," in Kalathil, Shanthi, ed., *Diplomacy, Development and Security in the Information Age*, Institute for the Study of Diplomacy, Georgetown, 2013.

FBI chief says Twitter-savvy ISIS poses bigger to US than al Qaeda. (n.d.). Retrieved November 23, 2015, from http://www.dailymail.co.uk/news/article-3172062/FBI-chief-reveals-Twitter-savvy-ISIS-poses-bigger-threat-old-fashioned-al-Qaeda.html

Gilsinan, Kathy. "Is ISIS's Social-Media Power Exaggerated?" *The Atlantic*. February 23, 2015.

Goudie, C., & Markoff, B. (n.d.). "ISIS recruiting US terrorists on social media." Retrieved November 23, 2015, from http://abc7chicago.com/534911/

Gonzalez, Richard. "CIA Director Pompeo Denounces WikiLeaks As 'Hostile Intelligence Service." *NPR*. April 23, 2017. http://www.npr.org/sections/thetwo-way/2017/04/13/523849965/cia-director-pompeo-denounces-wikileaks-as-hostile-intelligence-service

Grassegger, Hannes and Mikale Krogerus. “The Data That Turned the World Upside Down.” Motherboard. Retrieved January 31, 2017 from, http://motherboard.vice.com/read/big-data-cambridge-analytica-brexit-trump?

Grossman, Lev. “You — Yes, You — Are TIME's Person of the Year.” *Time Magazine*, December 25, 2006.

Hashemi, Tom. “The Business of Ideas is in trouble: Re-injecting Facts Into a Post-truth World.” *War on the Rocks*. December 9, 2016.

Hassan, Hind. “For millennials, by millennials: Startup Social Chain is taking social-media marketing to a new level.” Vice.com, February 26, 2015. https://news.vice.com/story/startup-social-chain-is-taking-social-media-marketing-to-a-new-level.

Heilbroner, Robert L. *Do Machines Make History?* in Smith, Merritt Roe and Leo Marx, eds. *Does Technology Drive History? The Dilemma of Technological Determinism.* Cambridge: The MIT Press, 1994.

Hippler, Thomas. *Bombing the People : Giulio Douhet and the Foundations of Air-power Strategy, 1884-1939*. Cambridge Military Histories, 2013.

Hoffer, Eric. *The True Believer; Thoughts on the Nature of Mass Movements.* New York: Harper and Row, 1951.

The Historical Roots and Stages in the Development of ISIS. (2015). Retrieved November 23, 2015, from http://www.crethiplethi.com/the-historical-roots-and-stages-in-the-development-of-isis/islamic-countries/syria-islamic-countries/2015/

Ignatius, David. “How ISIS Spread in the Middle East.” *The Atlantic*. October 29, 2015.

——— “Russia’s radical new strategy for information warfare.” *Washington Post*. January 18, 2017.

Infographic: Where Syria & Iraq’s Foreign Fighters Come From. (2015). Retrieved November 30, 2015, from /chart/3866/where-syria-and-iraqs-foreign-fighters-come-from/

"In Nations with Significant Muslim Populations, Much Disdain for ISIS." Pew Research Center. November 17, 2015. http://www.pewresearch.org/fact-tank/2015/11/17/in-nations-with-significant-muslim-populations-much-disdain-for-isis/.

Isachenkov, Vladimir. "Russia military acknowledges new branch: info warfare troops." AP News. February 22, 2017. https://www.apnews.com/8b7532462dd0495d9f756c9ae7d2ff3c/Russia-military-acknowledges-new-branch:-info-warfare-troops.

K. Thor Jensen, "Inside Donald Trump's Twitter-Bot Fan Club" *New York Magazine.* June 15, 2016. http://nymag.com/selectall/2016/06/inside-donald-trumps-twitter-bot-fan-club.html

Jowett, Garth, and Victoria O'Donnell. *Propaganda & Persuasion*. 5th ed. Thousand Oaks, Calif.: SAGE, 2012.

Kadushin, Charles. *Understanding social networks: Theories, concepts, and findings*. New York: Oxford University Press, 2012.

Kahneman, Daniel. *Thinking, Fast and Slow*. 1st ed. New York: Farrar, Straus and Giroux, 2011.

Kaine, Tim. "We're in the new age of information warfare ... and we're losing." Op-Ed, CNN.com. January 27, 2017.

Kalathil, Shanthi. "ICT, Political Transition, and the International Development Agenda." Lecture, CCTP-671 International Relations in the Information Age, Georgetown University, Washington, DC, October 26, 2015.

——— "Transparency and Volatility: International Relations in the Information Age," in Kalathil, Shanthi, ed., *Diplomacy, Development and Security in the Information Age*, Institute for the Study of Diplomacy, Georgetown, 2013.

Kaldor, Mary. *New and Old Wars: Organized Violence in a Global Era*. Stanford, Calif.: Stanford University Press, 1999.

Kaplan, Robert D. *Revenge of Geography*. Random House. Kindle ebook. 2012.

Katz, Rita. "The State Department's Twitter War With ISIS Is Embarrassing." *Time Magazine*, September 16, 2014.

Keohane, R. and Nye, J. “Power and Interpendence in the Information Age,” *Foreign Affairs*, Sept/Oct1998.

Khouri, Rami G. “Beware the hoax of countering violent extremism.” Al Jazeera America. September 29, 2015

Kilcullen, David. *Out of the Mountains : The Coming Age of the Urban Guerrilla*. New York: Oxford University Press, 2013.

Klapper, James. *The Effects of Mass Communication* New York: The Free Press, 1960

Kristof, Nicholas. “Bring Back Our Girls.” *The New York Times*. May 3, 2014. http://www.nytimes.com/2014/05/04/opinion/sunday/kristof-bring-back-our-girls.html?_r=0.

Kurtz, Judy. “White House Cribs 'Compton' Meme to Sell Iran Deal” TheHill. August 13, 2015. http://thehill.com/blogs/in-the-know/251071-white-house-cribs-compton-meme-to-sell-iran-deal#.

Lambeth, Benjamin S. *The Transformation of American Air Power*. Cornell Studies in Security Affairs. Ithaca, N.Y.: Cornell University Press, 2000.

Leggiero, Katherine. “Countering ISIS Recruitment in Western Nations.” *Journal of Political Risk*. January 3, 2015. http://www.jpolrisk.com/countering-western-recruitment-of-isis-fighters/.

Lubben, Alex "Twitter’s users are 15 percent robot, but that’s not necessarily a bad thing." VICE News, March 12, 2017.

Mackinlay, John. *The Insurgent Archipelago : From Mao to Bin Laden*. New York: Columbia University Press, 2009.

Mahan Alfred Thayer. *The Influence of Sea Power upon History, 1660-1783*, 5th ed. 1894; repr., Mineola, NY: Dover Publications, 1917.

Matsa, Katerina Eva and Kristine Lu. “10 facts about the changing digital news landscape.” Pew Research Center. September 14, 2016.

Mayer-Schönberger, Viktor, and Cukier, Kenneth, Author. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Mariner Books, 2014.

Mazzetti, Mark. *The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth*. New York: The Penguin Press, 2013.

Meet The Press: Thomas Freidman on the Russian interference in US election. *Meet the Press*, New York, NY: NBC Universal, March 5, 2017.

Mercy Corps. "Youth & Consequences: Unemployment, Injustice and Violence." 2015.

Meyer, Robinson. "War Goes Viral: How Social Media is Being Weaponized Across the World." *The Atlantic*. October 18, 2016.

Miller, Greg. "Panel Casts Doubt on U.S. Propaganda Efforts against ISIS." Washington Post.December 2, 2015. https://www.washingtonpost.com/world/national-security/panel-casts-doubt-on-us-propaganda-efforts-against-isis/2015/12/02/ab7f9a14-9851-11e5-94f0-9eeaff906ef3_story.html.

Mitchell, Malcolm. *Propaganda, Polls, and Public Opinion: Are the People Manipulated?* Englewood Cliffs, N.J.: Prentice-Hall, 1977.

Molla, Rani. "Social Studies: Twitter vs. Facebook." *Bloomberg Gadfly.* February 12, 2016. https://www.bloomberg.com/gadfly/articles/2016-02-12/social-studies-comparing-twitter-with-facebook-in-charts

Monroe, Alan D. *Public Opinion in America*. New York: Dodd, Mead, 1975.

Mullen, Jethro, "What is ISIS' appeal for young people?" CNN.com. February 25, 2015. http://www.cnn.com/2015/02/25/middleeast/isis-kids-propaganda/index.html

Nance, Malcolm. *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*. Skyhorse Publishing. Kindle edition, 2016.

Naylor, Seán D. "Airstrikes Killing Thousands of Islamic State Fighters, but It Just Recruits More." *Foreign Policy*, June 9, 2015.

Nye, Joseph “Soft Power: The Means to Success in World Politics.” Foreign Affairs. May/June 2004.

Olcott, Anthony. “Institutions and Information: The Challenge of the Six Vs.” ISD Working Paper in New Diplomacy. Institute for the Study of Diplomacy, Georgetown University, 2010.

Office of Director of National Intelligence. Report: “Assessing Russian Activities and Intentions in Recent US Elections.” January 6, 2017.

Ogene, Ashionye. “Abandonment of 'Bring Back Our Girls'” Al Jazeera English. October 14, 2014.

Ohanian, Alexis “How to make a splash in social media” 2009. TEDIndia. Film. http://www.ted.com/talks/alexis_ohanian_how_to_make_a_splash_in_social_media

Pandith, Farah, and Zarate, Juan. “Winning the War of Ideas.” Center for Strategic and International Studies. Accessed January 18, 2016. http://csis.org/files/publication/151116_Pandith_War_Ideas.pdf.

Paul, Christopher and Miriam Matthews. “The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It.” Santa Monica, CA: RAND Corporation, 2016.

“Pentagon Looks to Social Media as New Battlefield.” The Telegraph. July 21, 2011. http://www.telegraph.co.uk/technology/social-media/8651284/Pentagon-looks-to-social-media-as-new-battlefield.html.

Peterson, Andrea. “Three charts that explain how U.S. journalists use social media.” The Washington Post. May 06, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/05/06/three-charts-that-explain-how-u-s-journalists-use-social-media/?utm_term=.8cf0ce424f04.

Pomerantsev, Peter. “How Putin is Reinventing Warfare.” *Foreign Policy.* May 5, 2014.

Rabil, R. G. “The ISIS Chronicles: A History.” Retrieved November 23, 2015, from http://nationalinterest.org/feature/the-isis-chronicles-history-10895

Rid, Thomas. *Cyber War Will Not Take Place*. New York: Oxford University Press, 2013.

Reilly, Ryan J., FBI: When It Comes To @ISIS Terror, Retweets = Endorsements. (2015). Retrieved November 23, 2015, from http://www.huffingtonpost.com/entry/twitter-terrorism-fbi_55b7e25de4b0224d8834466e

Reilly, Ryan J. "If You're Trying To Join ISIS Through Twitter, The FBI Probably Knows About It." Huffington Post. July 9, 2015. http://www.huffingtonpost.com/2015/07/09/isis-twitter-fbi-islamic-state_n_7763992.html

Rosin, Hanna. "Among the Hillary Haters." *The Atlantic.* March 1, 2015.

Sanchez, Ray. "ISIS exploits social media to make inroads in U.S." CNN.com. June 4, 2015. http://www.cnn.com/2015/06/04/us/isis-social-media-recruits/index.html

Schmidt, Nadine and Tim Hume, "Berlin teen admits fabricating migrant gang-rape story, official says" CNN.com, February 1, 2016.

Senate Armed Services Committee. Russian Hacking and Cybersecurity Testimony. C-Span video. https://www.c-span.org/video/?420936-1/senior-intelligence-officials-resolute-russian-role-electionyear-hacking. January 5, 2017.

Senate Intelligence Committee Testimony, "Disinformation: A Primer In Russian Active Measures And Influence Campaigns" Clint Watts, March 30, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf

Schmitt, E. "U.S. Intensifies Effort to Blunt ISIS' Message." *The New York Times*. February 16, 2016. http://www.cnn.com/2016/02/01/europe/germany-teen-migrant-rape-false/

Scott-Joynt, Jeremy. "What Myspace means to Murdoch." BBC News Analysis. http://news.bbc.co.uk/2/hi/business/4697671.stm. July 19, 2005.

Sharma, Supriya. “Networking in the Market for Loyalties.” Lecture, CCTP-671 International Relations in the Information Age, Georgetown University, Washington, DC, November 16, 2015.

Shapiro, Ian. *Containment : Rebuilding a Strategy against Global Terror*. Princeton: Princeton University Press, 2007.

Shearer, Lee, Terrorists don’t fit profiles, partly because of social media recruiting, says federal analyst. (2015). Retrieved November 23, 2015, from http://onlineathens.com/mobile/2015-09-12/terrorists-dont-fit-profiles-partly-because-social-media-recruiting-says-federal

Shirky, Clay. “The Political Power of Social Media.” *Foreign Affairs*. December 20, 2011.

Siddiqui, Faiz and Susan Svrluga, “N.C. man told police he went to D.C. pizzeria with gun to investigate conspiracy theory.” *Washington Post*, December 5, 2017. https://www.washingtonpost.com/news/local/wp/2016/12/04/d-c-police-respond-to-report-of-a-man-with-a-gun-at-comet-ping-pong-restaurant/?utm_term=.0a3d97617630

Silverman, Craig. “This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook.” Buzzfeed News. November 16, 2016. https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.fagdJa5XE#.rrPkODZa8

Simmons, Beth. “International Relationships in the Information Age.” *International Studies Review*, 2013.

Simpson, Emile. “War and Peace in the Age of the Smartphone.” *Newsweek*. July 13, 2014.

Singer, P. W., and Friedman, Allan. *Cybersecurity and Cyberwar : What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Steven, Graeme C. S., and Gunaratna, Rohan. *Counterterrorism: A Reference Handbook*. Contemporary World Issues. Santa Barbara, Calif.: ABC-CLIO, 2004.

Stringfellow, Angela. “5 Hashtag Strategies To Boost Brand Awareness.” OPEN Forum. October 30, 2013.

https://www.americanexpress.com/us/small-business/openforum/articles/5-hashtag-strategies-to-boost-brand-awareness/.

Surowiecki, James. *The Wisdom of Crowds*. New York: Anchor Books, 2005.

Sun-tzu, Ralph D. Sawyer, and Mei-chiin Lee. *Sun Tzu: The Art of War*. Boulder, CO: Westview Press, 1994.

Syria-Iraq: The Islamic State militant group. BBC.com. Retrieved November 23, 2015, from http://www.bbc.com/news/world-middle-east-24179084

Swift, Art. "Americans' Trust in Mass Media Sinks to New Low." *Gallup*, September 14, 2016. http://www.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx

Tasch, Barbara. 'The aim is to weaken the West': The inside story of how Russian propagandists are waging war on Europe. *Business Insider*. February 2, 2017. http://www.businessinsider.com/russia-propaganda-campaign-weakening-europe-2017-1

Taylor , Phillip M. *Munitions of the Mind: A History of Propaganda*. Manchester University Press, 1995.

Theohary, Catherine and Cory Welt. 2017. *Russia and the U.S. Presidential Election*. CRS Report No. IN10635. Washington, DC: Congressional Research Service.

Timberg, Craig. "As a conservative Twitter user sleeps, his account is hard at work." The Washington Post. February 05, 2017. https://www.washingtonpost.com/business/economy/as-a-conservative-twitter-user-sleeps-his-account-is-hard-at-work/2017/02/05/18d5a532-df31-11e6-918c-99ede3c8cafa_story.html?tid=sm_tw&utm_term=.64127815c9ce.

"Terrorist Use of Social Media: Policy and Legal Challenges" DC Roundtable Forum. Council on Foreign Relations. October 14, 2015.

Thompson, Alex. "Parallel narratives: Clinton and Trump supporters really don't listen to each other on Twitter." Vice News, December

8, 2016. https://news.vice.com/story/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows

Townsend, Tess. "Meet the Romanian Trump Fan Behind a Major Fake News Site." Inc.com. November 21, 2016. http://www.inc.com/tess-townsend/ending-fed-trump-facebook.html

United States Department of State, Report: *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87*, Washington D.C.: Bureau of Public Affairs, August, 1987.

Waller, Michael J. "Strategic Influence: Public Diplomacy, Counterpropaganda, and Political Warfare." Washington, DC: Institute of World Politics Press, 2009.

Walt, Stephen M., "ISIS as Revolutionary State." *Foreign Policy,* November/December 2015: 42-51

Weimann, Gabriel. *Terrorism in Cyberspace : The next Generation*. Washington, D.C.: Woodrow Wilson Center Press, 2015.

Weston, J. Kael. *The Mirror Test: America at War in Iraq and Afghanistan*. New York: Penguin Random House, 2016.

Williams, Lauren "The FBI Doesn't Care If Your ISIS Retweet Wasn't An Endorsement." http://thinkprogress.org/justice/2015/09/19/3703465/isis-retweets-are-endorsements/

Wilson, Lydia. "What I Discovered From Interviewing Imprisoned ISIS Fighters." *The Nation*. October 21, 2015. http://www.thenation.com/article/what-i-discovered-from-interviewing-isis-prisoners/.

Withnal, Adam. "Nicolas Henin: The man who was held captive by Isis for 10 months says how they can be defeated" *The Independent*. December 2, 2015. http://www.independent.co.uk/news/world/middle-east/nicolas-henin-the-man-who-was-held-captive-by-isis-for-10-months-says-how-they-can-be-defeated-a6757336.html

Wood, Graeme. "What ISIS Really Wants." *The Atlantic*. March 2015.

Yan, Holly. “Why is ISIS so successful at luring Westerners?” CNN.com. March 23, 2015 http://www.cnn.com/2015/03/23/world/isis-luring-westerners/index.html

Zarrati, Sarra. “NGOs as protagonists in 21st century diplomacy.” Think IR Blog, United Kingdom, www.thinkir.co.uk, January 2015.

Zelin, Aaron. “Foreign Jihadists in Syria: Tracking Recruitment Networks.” (n.d.). Retrieved November 30, 2015, from https://www.washingtoninstitute.org/policy-analysis/view/foreign-jihadists-in-syria-tracking-recruitment-networks.